International Journal of Computations, Information and Manufacturing

Volume.2, Issue.2, 2022

Editors-in-Chief
Prof. Haitham M. Alzoubi and Dr. Taher M. Ghazal

Global Academic Forum
on Technology, Innovation and Management

gaftim.com

Online at: https://journals.gaftim.com/index.php/ijcim/issue/view/ 7

Editors-in-Chief

Associate Editors

Editorial Board

EDITORIAL

The necessity of technology has embraced the significance of research and knowledge for everyone. It's a stretch to bring the impression into the academic world as well in this advanced technological era, where things have transformed drastically in all existing domains evolving the variation all over the globe. As we know, the use of technology in developing computation, innovation, and manufacturing overall plays a significant role. We acknowledge the efforts of diligent researchers who are great contributors to the accomplishment of providing vast knowledge in the domains of computation, innovation, and manufacturing globally through this journal.

IJCIM develops highly innovative computer and information science technologies research to provide creative solutions for various manufacturing businesses, known as computer sciences, information technology, and manufacturing. IJCIM is a global site for the publication of excellent, high quality, peer-reviewed papers by scientists and engineers working in all the domains of computation, innovation, and manufacturing technologies.

The editorial board of IJ-CIM are pleased to introduce the second issue of the second volume to 2022 year of the “International Journal of Computations, Information and Manufacturing” (IJCIM). The IJCIM is published by Global Academic Forum on Technology, Innovation and Management (GAF-TIM).

The inaugural of issue2, volume2, of IJCIM includes six articles. In this issue, the opening with a literature survey of security and privacy issues in internet of medical things. Followed by an investigating e-supply chain issues in internet of medical things (IoMT): evidence from the healthcare. Moreover, a systematic review of blockchain technology use in e-supply chain in internet of medical things (IoMT) has been discussed. Along with stakeholders' perspectives on wearable internet of medical things privacy and security. Conducting a systematic review on security vulnerabilities to preveny types of attacks in IoMT presented as well.

IJCIM appreciates all the support that it is receiving from its members as well as from its readers.

Editors-in-Chief
Prof. Haitham M. Alzoubi* and *Dr. Taher M. Ghazal

A LITERATURE SURVEY OF SECURITY AND PRIVACY ISSUES IN INTERNET OF MEDICAL THINGS

Jesus Cuauhtemoc Tellez Gaytan

Associate Professor of Finance, Business School, Tecnologico de Monterrey, Mexico

cuauhtemoc.tellez@tec.mx

ABSTRACT

A technology answer to the world's health concerns, ubiquitous healthcare is being considered. A combination of rising healthcare expenses and a growing demand for high-quality medical care has led to this. The development of the Internet of Things (IoT) has a greater impact on IoMT. Improved health care and safety are being provided to millions of people worldwide as a result of the Internet of Things (IoMT). Remote monitoring and transfer of data can provide medical data centres, such as those in the cloud, with real-time access to patient health characteristics. As a result, healthcare is more accessible, more effective, and less expensive. It's a problem, however, because of the proliferation of Internet of Things devices. This poses a problem because IoMT devices are compact and have a limited number of schemes and computing power. It is challenging to administer and safeguard IoMT systems because of their widespread use. This is amajor problem that prevents the therapeutic application of IoMT. Internet of Things (IoT)security issues, threats, requirements, and potential future research are all covered in this report. Existing solutions and unresolved issues in the realms of security and privacy are also receiving considerable attention. This paper provides a general overview of the various art techniques by using a recognised solution.

Keywords:Internet of Medical Things, Security, Privacy, Healthcare

Online: https://doi.org/10.54489/ijcim.v2i2.106 Publisher: **GAF-TIM**, https://gaftim.com

1. INTRODUCTION

It is expected that healthcare practitioners would benefit greatly from the wide range of applications of the Internet of Things. Wearable, implantable, and intelligent medical gadgets have all seen a recent uptick in popularity. Biosensors, materials, and microelectronics have made this possible. Security issues in IoMT-based healthcare systems have received less attention. Patients' privacy could be at risk if IoMT health care systems are not effectively protected [1], [2]. IoMT devices identify life-threatening events late and inaccurately as a result of DoS attacks. HP Fortify's 2015 study of popular smart watches found eleven security weaknesses, including authentication problems, privacy concerns, unsafe software, and a lack of authorization [3]. A good example of this is the authentication process, which verifies a user's identity in some way. IoMT healthcare systems should only be accessible to authorised devices and users [4], [5]. If a user's sensitive healthcare information is not adequately protected, attackers can quickly gain access to it. Patient data must be protected by using authentication to ensure that only authorised individuals and organisations have access to it . Patients' medical records are therefore restricted to those who have been verified through the Authentication process [6]. In the world of computer systems and networks, system and network security are well-known issues and methodologies. Examples of digital signature algorithms include DSA, RSA, and other public-key cryptosystems. However, many of these cryptosystems are inefficient for IoT devices due to their low processing power and power consumption [7]. Because implanted medical devices have lower battery capacity than IoT devices, they are less effective in ensuring their wearers' health. IoMT devices can store and process health data, for instance [8]. Therefore, these devices must be more secure than typical Internet of Things (IoT) and personal computers. Security and safety issues are frequently overlooked by healthcare systems utilising the Internet of Things (IoMT) [9].

1.1 Problem definition

The healthcare IoMT system has been subjected to a security audit. In addition, the cryptosystem's main components, such as the random number generator (RNG), will be examined in detail. Examples include RNG research on IoMT devices [10]. Finally, a presentation on the security plans for implantable IoMT social insurance gadgets and an audit of biometric verification in the human services systems will be given [11]. Asymmetrical (public-key) and symmetrical cryptography are the two main cryptographic pseudocode and method for secure encryption. In comparison to symmetric encryption, asymmetric encryption is more secure, but itis more difficult to implement since it requires more computational power [12]. An overhead communication channel should be reduced and any information encryption and decoding methods provided for testing IoMT contraptions should be light-weight due to the limited compute capability of sensor-level devices. Web-based communications, such as those between medical professionals and their patients, necessitate a much more robust security framework to protect sensitive information [13]

1.2 Proposed solution

An overview of new requirements for IoMT healthcare systems' privacy and security is provided in this document, which outlines the new requirements [14]. Research methods such as surveys and reviews are among the many described in this article [15]. Data flow in IoMT systems must be secure and private, according to a study by Mohamed Shakeel et al. (2018) [16]. Singh & Tomar (2018) reviewed the linked vulnerabilities in the IoHT environment on medical devices. It's important to note that examined privacy preservation challenges in the context of the healthcare environment [17]. A study, that ranked and categorised the best security research based on insolent healthcare systems [18], [19]. For the purposes of this study, the IoMT-based healthcare system's data is examined all the way up to the medical server using a bottom-up approach that focuses on privacy and security. In addition, this research proposes a biometric technique that could be used to maintain IoMT healthcare systems secure.

2. LITERATURE REVIEW

The IoMT healthcare system's cryptography designs, applications, and security evaluations are examined in detail. Random number generation, for example, will be examined in great detail because it is one of the most critical components of the cryptographic system (RNG) [20]. Anillustration of this is the study of RNG in IoMT devices. The survey results on implanted IoMT social insurance device security plans and an evaluation of human services biometric verification systems will also be reviewed [21], [22].

There are two types of public-key encryption: asymmetrical and symmetrical [23]. It takes more computing power to encrypt with asymmetric encryption than symmetric encryption, but it is more secure [24]. Any information encryption and decoding methods used for testing IoMT contraptions should be light-weight because sensor-level devices have limited computational capability [25]. Data shared on open networks, such as the internet, should be protected with more robust security measures; for example, communications between medical specialists and patients should not be intercepted [26], [27].

Most cloud-based authentication, access control research, and data storage use symmetric cryptography [28]. Because of its large keys, elliptic curve cryptography (ECC) is the most accessiblepublic-critical algorithm [29], [30]. Among the most notable examples is River-Shamir-Adleman (RSA) [31]. Hybrid-security systems frequently use symmetric pseudocodes as session keys because of their minimal weight and resource constraints [32]–[35]. Eavesdropping and replay, the Chosen Plain Text Attack (CPA), and impersonation are among the most popular attacks in security analysis. Attacks on hardware and computer simulations were used in tandem to disrupt the network [36].

To generate pseudo-random numbers, current computers use random seeding (PRNGs). The PRNG will always generate the same random integers if the seed is the same [37], [38]. If the seed of the PRNG is generated using a false random integer, malicious characters can attack the PRNG [39]. Several IoT devices include random number generators that are too large to be employed as sensors because of their limited power and size constraints [40]. Researchers must devise a way to create truly random numbers using inertial sensors in IoMT devices [41].

System components like sensors, medical servers, and personal servers all feature in IoMT-basedhealthcare [42], [43]. The IoMT healthcare plan design has lately incorporated a wide range of healthcare systems into its design [44]. Body Sensor Network (BSN) is a network of sensors and medicaldevices at the sensor level (BSN). RFID, NFC, and Bluetooth Low Energy, three types of wireless communication technology, are used by sensors and personal servers (BLE) [45], [46]. BLE, unlike RFID and NFC, offers a wide range of network topologies, including mesh and star [80], which are crucial for implanted devices. In the year of our Lord 201 [47].

Personal servers get physiological data from medical devices [48]. Examples of devices that could be used as servers include tablets and smartphones [49]. Before a patient's data can be delivered to an integrated medical server, it must be processed and stored on a personal server [50], [51]. A personal serveris necessary when a network connection to a medical server is lost since it can continue to operate [52]. Patients' medical records can be accessed quickly and easily by medical professionals. The patient's agreement is required for the use of computer programmes and algorithms, as well as medical servers, for early rehabilitation and diagnosis progress evaluations [53]. Over the past few decades, numerous IoMT systems have pushed the idea of constant patient monitoring 78 [21], [54], [55]. As a result, many of them lack privacy and security safeguards. In these investigations, researchers have concentrated on the utility and consumption of electricity, rather than the security and privacy of patient data [56]. An IoMT healthcare system called BSN-Care recently included authentication and encryption features.

3. RESEARCH METHODOLOGY

Secondary study was utilised to investigate Ethics and Security Issues in Internet of Medical Things (IoMT. In order to analyse the data, a theme approach was used. The term "desk research" refers to the fact that this type of study is done at the researcher's desk. In this type of study, information that has already been acquired is utilised. After that, the existing data is analysed and structured in a way that enhances the research's overall effectiveness. The internet, government records and resources, libraries, and other studies are some of the many sites where data can be found. Secondary research is more cost-effective than primary research since primaryresearch tends to be more expensive. As a result, secondary research relies on previouslygathered data, while primary research relies on data collected by the researcher or by someone else acting as an agent of the researcher. In addition to primary research methods, such as cati surveys and online surveys, secondary research can be utilised to enhance the data collected through these methods.

4. DISCUSSION

In this research, wireless connectivity and internet-based IoMT technologies pose major privacy and security risks to the future generation of medical devices. Devices that constantly monitor patients, rather than safeguarding medical equipment at laboratories and wards, are implanted in patient. As a result, IoMT devices can better handle the sensitive personal and physiological data they collect from their users. This was a risky approach because the attack surface and severity were both raised in comparison to previous IoT systems. Some examples are nerve stimulators, insulin pumps, and heart rate monitors. If these devices are not sufficiently safeguarded from malicious attacks, patients' lives could be at jeopardy. Furthermore, Radcliff demonstrated that he was able to hack an insulin pump and even instruct it to inject the wrong amount of insulin.

New strategies and approaches are always being devised in order to penetrate a network. As a result, government institutions must employ antivirus software and keep it up to date in order to protect their systems against hacker attacks. Implantable medical devices are hindered by a lack of resources and a network capable of regularly updating their firmware, unlike computernetworks where virus updates may be quickly implemented by injecting software into thesystem. In the event of a malicious attack, these medical devices can't be shut down, therefore they must wait for a security expert to identify an antivirus. Biometric authentication is a growing source of worry for IoMT security and privacy. It hasn't been embraced because of its drawbacks, such as inadequate authentication performance and high sensor costs.. Because most medical devices capture physiological data from their users (such as heart rate and blood pressure), biometric authentication is advantageous.

5. CONCLUSION

Since the development of wearable and implanted medical devices, the number of IoMT devices in the healthcare sector has increased significantly. A few examples of innovative medical equipment with embedded technologies are insulin pumps, air quality sensors, sleep monitors, and drug efficacy tracking systems. There are many instances of how these new methods have benefited healthcare, but two stand out: prevention and treatment modification. These devices have artificial intelligence built in to keep hackers and the patients they're monitoring away. Due to the simplicity with which they can be controlled and monitored across a network, these devices can potentially be targeted directly or indirectly. Because these IoMT gadgets handle highly personal data and some of the gadgets that run on autonomic functions, attacks on them could be directly and life-threatening to the users running on them. The system analyst is in charge of backing up the data of their users and making certain that only those with the proper credentials have access to the relevant control rooms and network components. Wi-Fi networks must also have a firewall to secure their internet connectivity.

Security solutions could protect the user and medical devices against IoMT device vulnerabilities. The small size and restricted capacity of wearable and implantable electronics limit their resources and security measures in times of disaster. We need new and improvised approaches to safeguard these gadgets in the hospital setting that span all aspects of human-computer interaction as well as physical deployment. New standards must be developed in close collaboration with business, healthcare facilities, academic institutions, and governmental organisations if they are to suit the demands of both users and creators.

REFERENCES

[1] C. Verikoukis, “Review of Security and Privacy for the Internet of Medical Things (IoMT) Resolving the protection concerns for the novel circular economy bioinformatics,” *2019 15th Int. Conf. Distrib. Comput. Sens. Syst.*, pp. 457–464, doi: 10.1109/DCOSS.2019.00091.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] F. Alsubaei and S. Shiva, “Security and Privacy in the Internet of Medical Things : Taxonomy and Risk Assessment,” no. 6, pp. 112–120, 2017, doi: 10.1109/LCN.Workshops.2017.72.

[7] 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.

[8] 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.

[9] F. Alsubaei, A. Abuhussein, and S. Shiva, *A Framework for Ranking IoMT Solutions Based on Measuring Security and Privacy*, vol. 2. Springer International Publishing, 2019. doi: 10.1007/978-3-030-02686-8.

[10] 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.

[11] 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.

[12] 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.

[13] J. Almalki *et al.*, “Enabling Blockchain with IoMT Devices for Healthcare,” *Information*, vol. 13, no. 10, p. 448, 2022, doi: 10.3390/info13100448.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] F. Ma, T. Sun, L. Liu, and H. Jing, “Detection and diagnosis of chronic kidney disease using deep learning-based heterogeneous modified artificial neural network,” *Futur. Gener. Comput. Syst.*, vol. 111, pp. 17–26, Oct. 2020, doi: 10.1016/j.future.2020.04.036.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] Y. Sun, F. P. Lo, and B. Lo, “Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems : A Survey,” *IEEE Access*, vol. 7, pp. 183339–183355, 2019, doi:

10.1109/ACCESS.2019.2960617.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] G. M. Qasaimeh and H. E. Jaradeh, “THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE EFFECTIVE APPLYING OF CYBER GOVERNANCE IN JORDANIAN COMMERCIAL BANKS,” *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, 2022.

[34] 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.

[35] 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.

[36] T. M. Ghazal *et al.*, “IoMT Cloud-Based Intelligent Prediction of Breast Cancer Stages Empowered with Deep Learning,” *IEEE Access*, vol. 9, pp. 146478–146491, Oct. 2021, doi: 10.1109/ACCESS.2021.3123472.

[37] 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.

[38] 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.

[39] 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.

[40] H. M. Alzoubi and Y. Ramakrishna, “Empirical Investigation of Mediating Role of Six Sigma Approach in Rationalizing the COQ in Service Organizations,” *Oper. Supply Chain Manag.*, vol. 15, no. 1, pp. 122–135, 2022, doi: 10.31387/oscm0480335.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

[46] 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.

[47] M. Abdel-Basset, G. Manogaran, and M. Mohamed, “Internet of Things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems,” *Futur. Gener. Comput. Syst.*, vol. 86, pp. 614–628, 2018, doi: 10.1016/j.future.2018.04.051.

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] 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.

[56] 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.

INVESTIGATING E-SUPPLY CHAIN ISSUES IN INTERNET OF MEDICAL THINGS (IOMT): EVIDENCE FROM THE HEALTHCARE

Sasho Guergov

Technical University of Sofia, Bulgaria

Sguergov@tu-sofia.bg

ABSTRACT

The E-supply chain in the Internet of Medical Things is plagued by a number of problems. These problems include failing to meet patient expectations, keeping services and equipment affordable, and lacking adequate infrastructure management, cyber security, and network dependability. The research suggests various remedies that might be beneficial for these problems. In this study, the past literature is discussed in order to provide a general picture of the subject. The majority of the survey responses, which were used to run an SPSS test, agreed with the research hypotheses. The research is based on five hypotheses, and the SPSS test found empirical evidence respectively.

Keywords**:** E-Supply chain, Internet of Medical Things (IoMT), Healthcare.

1. INTRODUCTION

The Internet of Medical Things refers to a collection of medical applications and medical devices that connect to IT systems in healthcare through computer networks. Some wi-fi-equipped medical devices that allow machine-to-machine communication is the base of the IoMT [1]. IoMT is also known as Healthcare IoT. The e-Supply chain is used in the healthcare industry for various reasons, such as supporting and monitoring the medicine flow, medical equipment and supplies and providing the medical-related services from the Manufacturer to patients where IoMT plays a crucial role [2], [3]. The e-supply chain which is used in the medical industry contains some issues [4]. The issues are matching the expectation of the patients, keeping the service and the equipment cost-effective and Inadequacy in the infrastructure management [5]. In addition to this, the E-supply chain must face various

Online: https://doi.org/10.54489/ijcim.v2i2.110 Publisher: **GAF-TIM**, https://gaftim.com

technical challenges in the healthcare industry, such as challenges related to cyber security and reliability in the network [6], [7].

All these issues are significant for the healthcare industry. If there are some issues in the management and the requirements of the customers are not met, the treatment would not be in the proper way, the application of the e-supply chain is a costly process [8], so it is a big challenge for the e-supply chain management to keep the service cost-effective to the patient [9]. On the other hand, as the E-supply chain is fully dependent on the internet, the management must provide cyber security to the patients. Nowadays, cyber security issues are a big challenge [10], [11]. Also, the network from which the service is being availed should be reliable to the customers; in most cases, the management fails to provide network reliability to the patients [12].

1.1 Problem Definition

In this part of the paper, the problems of the E-Supply chain in the IoMT will be elaborated on in brief. Matching the expectation of the patients- Sometimes, it is very difficult to meet the patients' expectations through the E-supply chain. As it is said earlier, the usage of e-commerce is increasing in the IoMT [13]. Many patients are unfamiliar with e-commerce and the Internet of Things, which creates issues in meeting patients' requirements. In the healthcare industry, a patient's requirement is considered as the most important factor.

Keeping the system cost-effective- as it is said earlier, the implementation of the e-supply chain in the healthcare industry is a costly process which makes the services and equipment costs for the patient [14]. Now it is a big challenge for the service provider to provide a cost-effective service to the patients. This issue is important because it is hard to afford such costly services for patients from lower economic segments. To make the service available to all the patients, it must keep cost-effective [15].

Inadequate Infrastructure Management- In each service, the infrastructure is considered the most important factor [16]. If the infrastructure is not good, the service could not be satisfactory. Sometimes patients could not avail the Internet of Medical Things due to inadequate infrastructure management [17].

Cyber security is one of the biggest issues around the world. Especially for those services which are provided through the internet, cyber security is very much important. E-supply chain management relies on the transmission of a vast array of data [18]. The E-Supply chain in the healthcare industry is a long chain of services from the manufacturers to the patients. In the whole chain, there are various steps to be covered which opens the chances of security breaches [19]. There are various security issues which could arrive in the whole process. In the case of IoMT, the main challenge is to keep the patients' data secret [20]. The hackers could access the patients' data, such as their bank details and many more, which could be threatful to the patient [21].

Network reliability- The network reliability is another technical issue related to the E-Supply chain management [22], [23]. The e-supply chain in the IoMT depends on reliable information transmission from all factors of the e-supply chain; this process depends on reliable broadband access [24]. If the network is not reliable to the patients, the patients would not be able to avail of the service through the E-Supply Chain.

1.2 Proposed Solution

Solutions related to the problem of matching the expectation of the patients- The only way to meet the expectation and requirements of the patients is to deliver exactly those products or services that are promised [25]. Similarly, if the manufacturers or the service providers could lower the delivery time, the patients get satisfied [26]. Besides these factors, product and service satisfaction is another important factor [27]. If a patient gets satisfactory output from the service provider and if the service provider treats the patient with care and appears with an amicable behaviour, the service provider could meet the patient's expectations [28].

Solutions related to the problem of cost-effectiveness- To keep the service cost-effective, the service provider could take a just-in-time delivery model [29]. In this process, the manufacturers would manufacture only the ordered quantity. On the other hand, the service provider should try to reduce the internet cost to keep the service cost-effective to the patients [30]. Solutions related to the problem of inadequacy in infrastructure management- As it is said earlier, infrastructure management plays a crucial role in the E-Supply chain. If the manufacturers do not manage their infrastructure, it will not work. Especially for the IoMT, infrastructure is very important [31]. To solve the problems related to infrastructure management, the manufacturers could introduce the Warehouse Management Systems, which will help to manage the warehouse. Similarly, the service providers should develop the software to provide proper and promised service to the patients [32].

Solutions related to the problem of cyber security- E-supply chain systems can be affected by hackers at any time [33], [34]. The patients make payments through their cards which could be hacked. To prevent the cyber-attack, organizations take various steps, such as employing solutions that have the power of behavioral-based analysis. Indicators of Attacks (IOAs) could be the solution to it [35]. The IOAs will mitigate the risk of cyber-attacks. Another solution could be Threat Intelligence [36], [37]. Threat Intelligence could help the service providers when the entire system could be hacked [38]. Also, it will help to understand the types of attacks [39]. Falcone is an automated threat analysis tool that could be used for this purpose [40].

Solution related to the issue of network reliability- The issue of network reliability is another big issue in the E-Supply chain in IoMT [41], [42]. In order to fix the network reliability issue, the service provider could adopt some steps, such as- the can evaluate their current network setup so that it becomes smooth and fast [43], identifying the opportunities for up-gradation so that their network gets upgraded when it is required and preparing the network for future needs so that their network always remain available to the patients.

2. LITERATURE REVIEW

2.1 Issues related to infrastructure management

As identified in pas studies, there are various issues related to infrastructure management in the E-Supply chain system. According to Almalki, the supply chain infrastructure is at high risk, and it could lead to loss of the customer service, financial losses and many more [44]. A warehouse which is planned strategically could be a solution to this issue. The mobile apps of the company need to be developed and ensured it is working flawlessly [45], [46].

2.2 Issues related to the patient's requirements

The entire process of the supply chain has been re-shaped, and the competition in the market is increasing [47]. In this situation, meeting the expectation of the customers is necessary for the manufacturers [48]. Regarding the E-supply chain in IoMT, the manufacturers and the service providers must be cautious about those matters, and they should take such steps so that their service and the medical product can meet the requirements of the patients [49].

2.3 Issues related to cyber security

As it is discussed in the paper, the e-supply chain in the IoMT consists of the risk of cyber-attacks. As cited by various authors, there are various ways to perform web-attacks; those are- Trojans, potentially Unwanted Applications, fraudulent advertising, web spam, redirection of the browser and many more [50], [51]. In the case of IoMT, the patients could be attacked in these ways. These vulnerabilities could be prevented by securing the website and employing various tools [52].

2.4 Issues related to network reliability

According to prior investigation, the business which is employed with the e-commerce supply chain depends on reliable access to a broadband connection [53]. Any network downtime and power outages could lead to serious issues in the entire supply chain [54]. To mitigate these issues, the service providers need to fix the reliability of the network and the connection [55], [56].

This research paper would define the issues and provide a proposed solution and a survey report according to the issues related to the e-supply chain in the IoMT.

- **H^0**: Meeting the requirements of the patients is one of the issues for the e-supply chain in IoMT.
- **H^1**: Cost-effectiveness of e-supply chain implementation is another issue for IoMT.
- **H**^{2}: Inadequate Infrastructure management is a crucial issue for the E-Supply chain in the IoMT.
- **H^3**: Cyber security threat is a problem in implementing the e-supply chain in the IoMT.
- **H^4**: If there is no reliability in the network, Issues could arise in the e-supply chain for the IoMT.

3. RESEARCH METHODOLOGY

In the research method, there are five Hypothesis was tested; those are- Meeting the requirements of the patients is one of the issues for the e-supply chain in IoMT, Cost-effectiveness of e-supply chain implementation is another issue for IoMT, Inadequate Infrastructure management is a crucial issue for the E-Supply chain in the IoMT, Threat to Cyber security is a problem in implementing the e-supply chain in the IoMT, If there is no reliability in the network, Issues could arise in the e-supply chain for the IoMT.

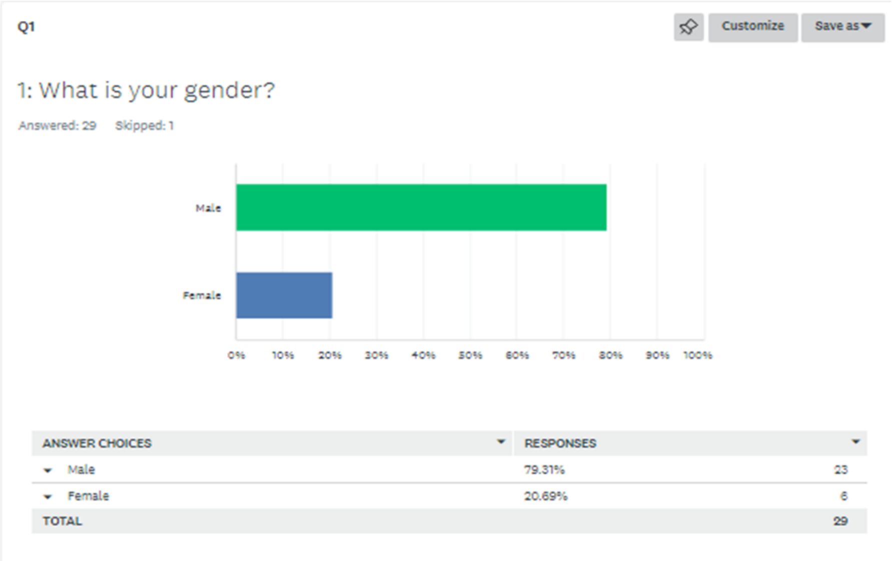
As the research methodology, a quantitative data analysis method has been used. This provides the statistical data. In this research method, there are one independent variable and two dependent variables. The independent variable is the E-Supply Chain Issues on Internet of Medical Things (IoMT), and two dependent variables are- Impact of the patients' satisfaction and the Impact of the Infrastructure management.

In the path of conducting this research, a random survey is done. A questionnaire consisting of 10 questions was presented to 30 random people associated with the healthcare sector in the UAE. The ten questions of the questionnaire related to the hypothesis. Using this survey method, 30 different reactions of people from different age groups have been collected . This survey helped to understand the impact and significance of the issues. If the qualitative data analysis method through some interviews could have been used, it would only get the reaction and opinions of those persons. On the other hand, through the survey method, the research has been able to achieve the reaction of 30 different people. It can be said that the survey method is fruitful for such research, and through the survey method, the hypotheses are tested strategically.

4. DATA ANALYSIS

4.1 Survey Result

1: What is your gender?



Q1

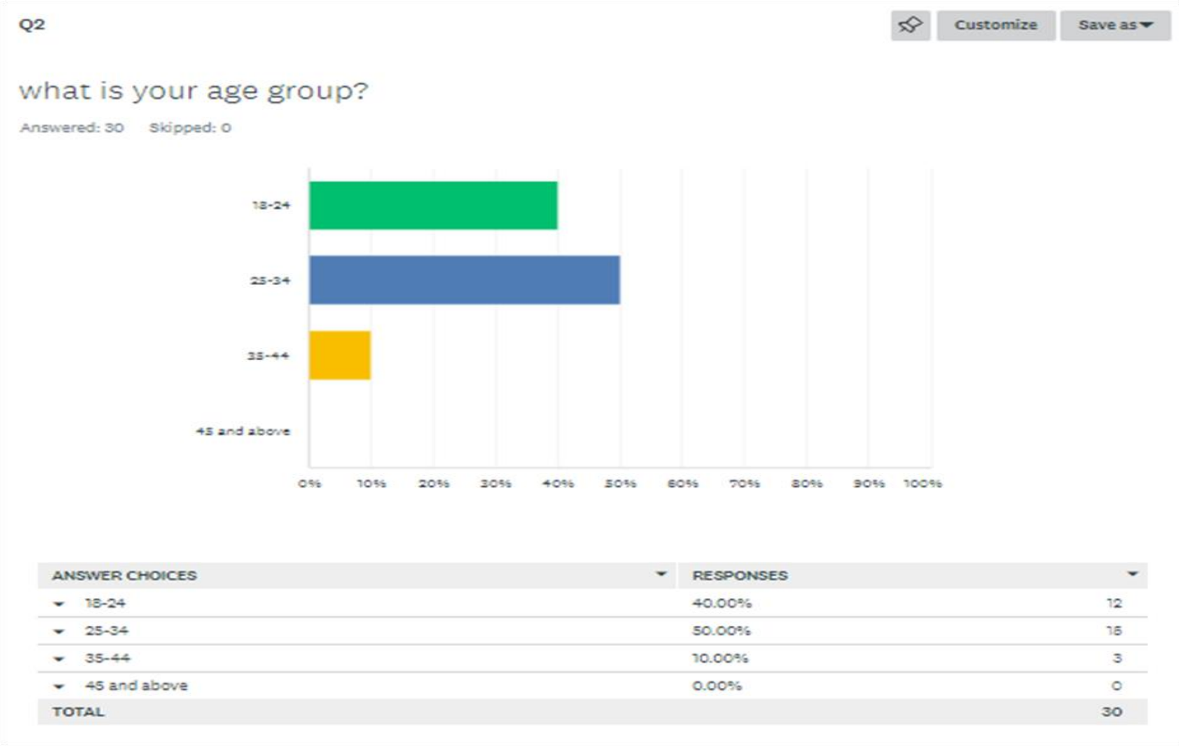
1: What is your gender?

Answered: 29 Skipped: 1

ANSWER CHOICES	RESPONSES	
Male	79.31%	23
Female	20.69%	6
TOTAL		29

In this question, it is seen that almost 80 per cent of the people are male . Most of the reaction is collected from males.

2: What is your age group?



Q2

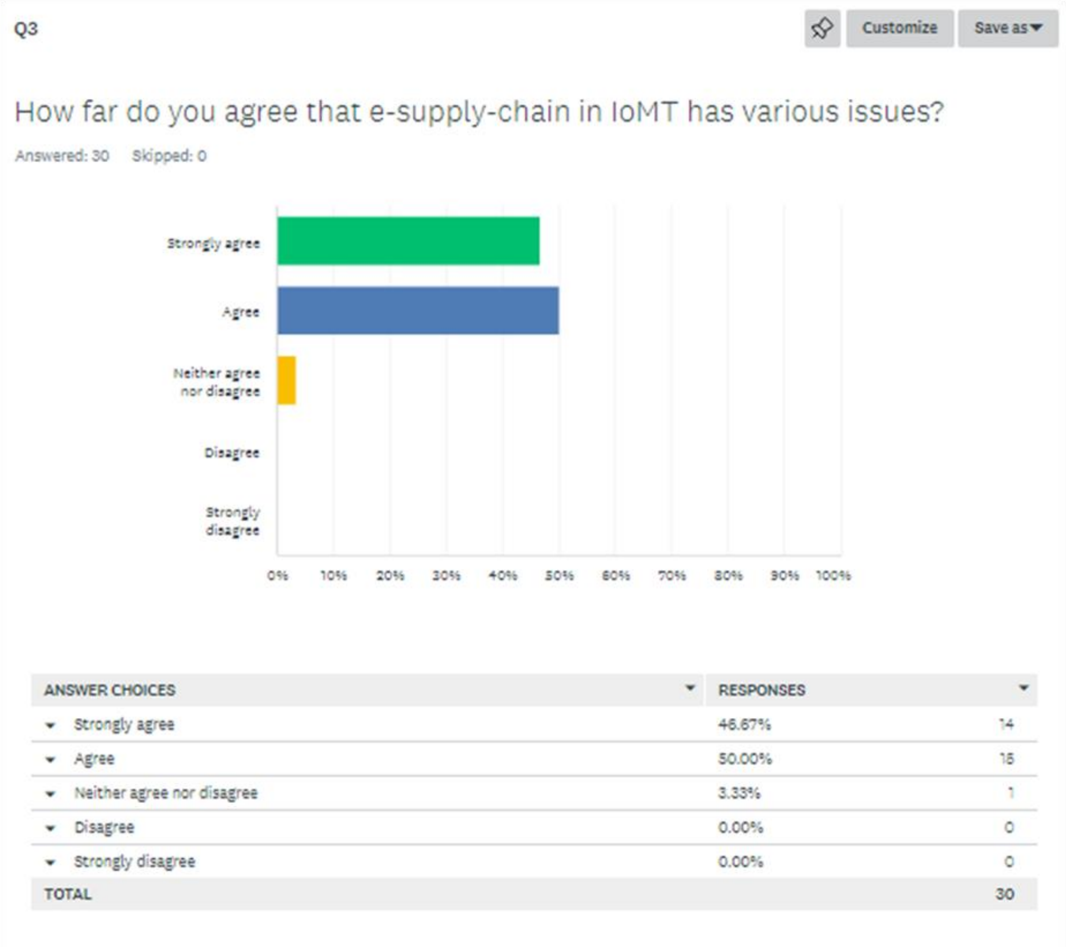
what is your age group?

Answered: 30 Skipped: 0

ANSWER CHOICES	RESPONSES	
18-24	40.00%	12
25-34	50.00%	15
35-44	10.00%	3
45 and above	0.00%	0
TOTAL		30

In this survey, the respondents are from multiple age groups and through this it is understood that people of various age groups are aware about this, mainly the younger generation.

3: How far do you agree that the supply chain in IoMT has various issues?



Q3

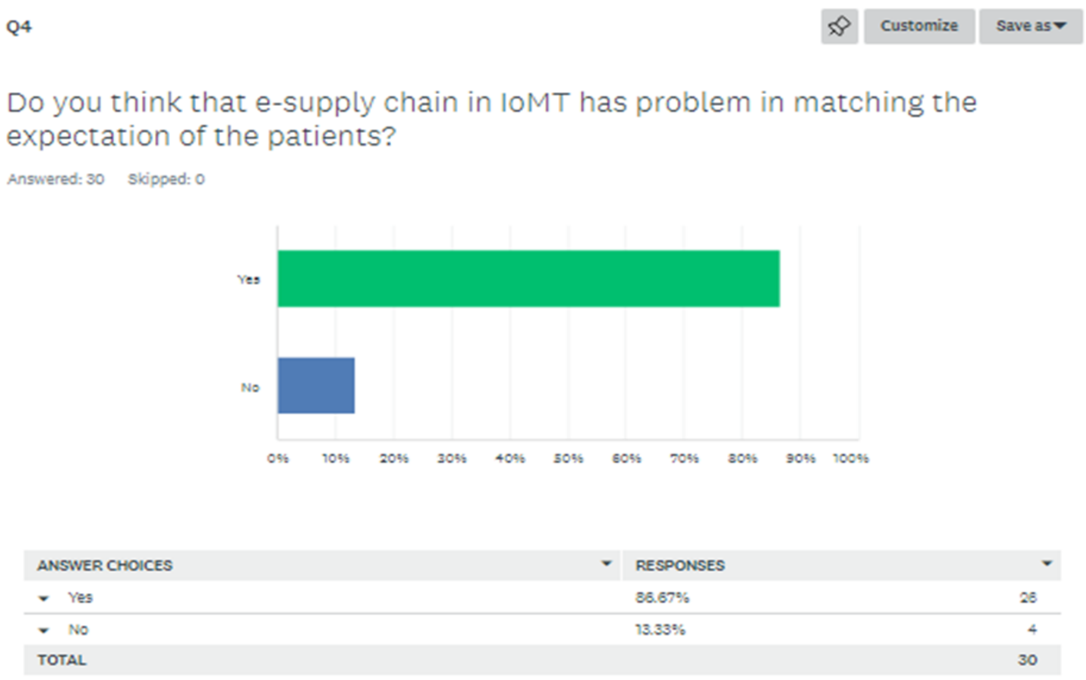
How far do you agree that e-supply-chain in IoMT has various issues?

Answered: 30 Skipped: 0

ANSWER CHOICES	RESPONSES	
Strongly agree	46.67%	14
Agree	50.00%	15
Neither agree nor disagree	3.33%	1
Disagree	0.00%	0
Strongly disagree	0.00%	0
TOTAL		30

In question no. 3; almost 46 per cent of people strongly agreed, and 50 per cent of the people agreed that the e-supply chain has several issues in the IoMT. The e-supply chain has a real issue with the IoMT.

4: Do you think that the e-supply chain in IoMT has a problem in matching the expectation of the patients?



Q4

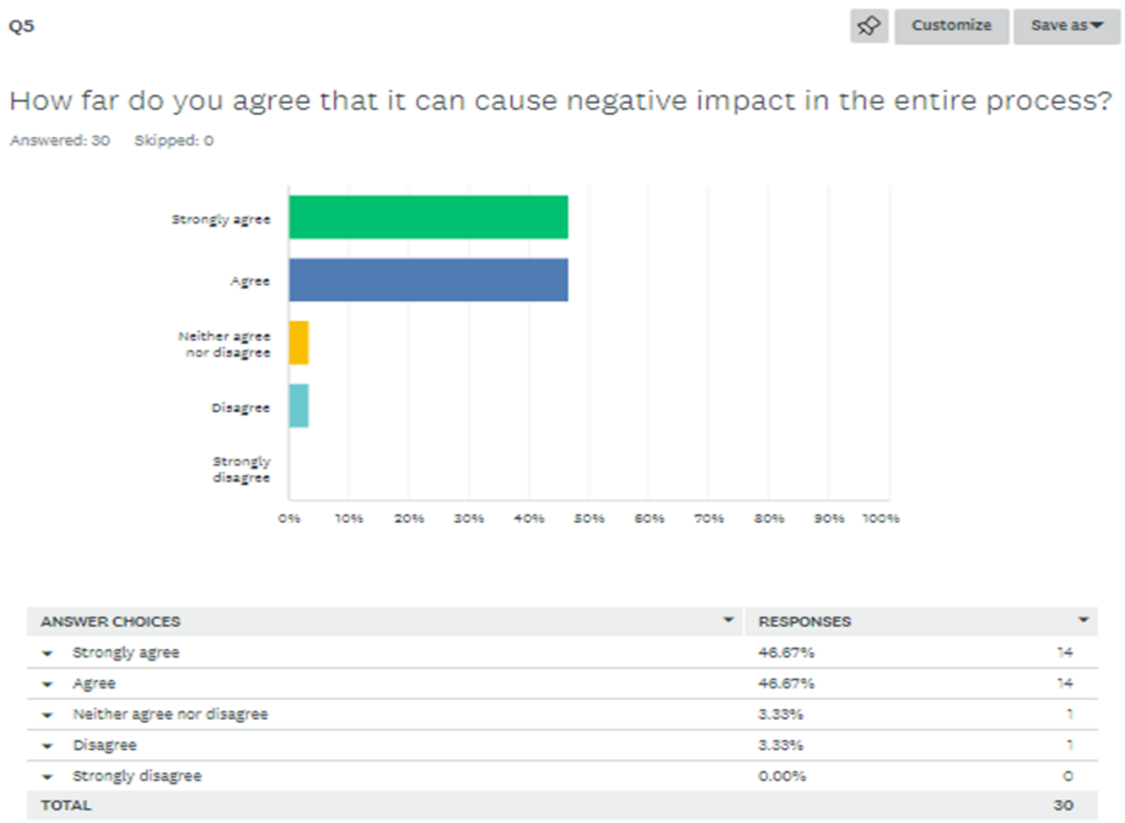
Do you think that e-supply chain in IoMT has problem in matching the expectation of the patients?

Answered: 30 Skipped: 0

ANSWER CHOICES	RESPONSES	
Yes	86.67%	26
No	13.33%	4
TOTAL		30

Among 30 people, 26 people think that the E-supply chain fails to match the customers' expectations in the IoMT.

5: How far do you agree that it can cause a negative impact in the entire process?



Q5

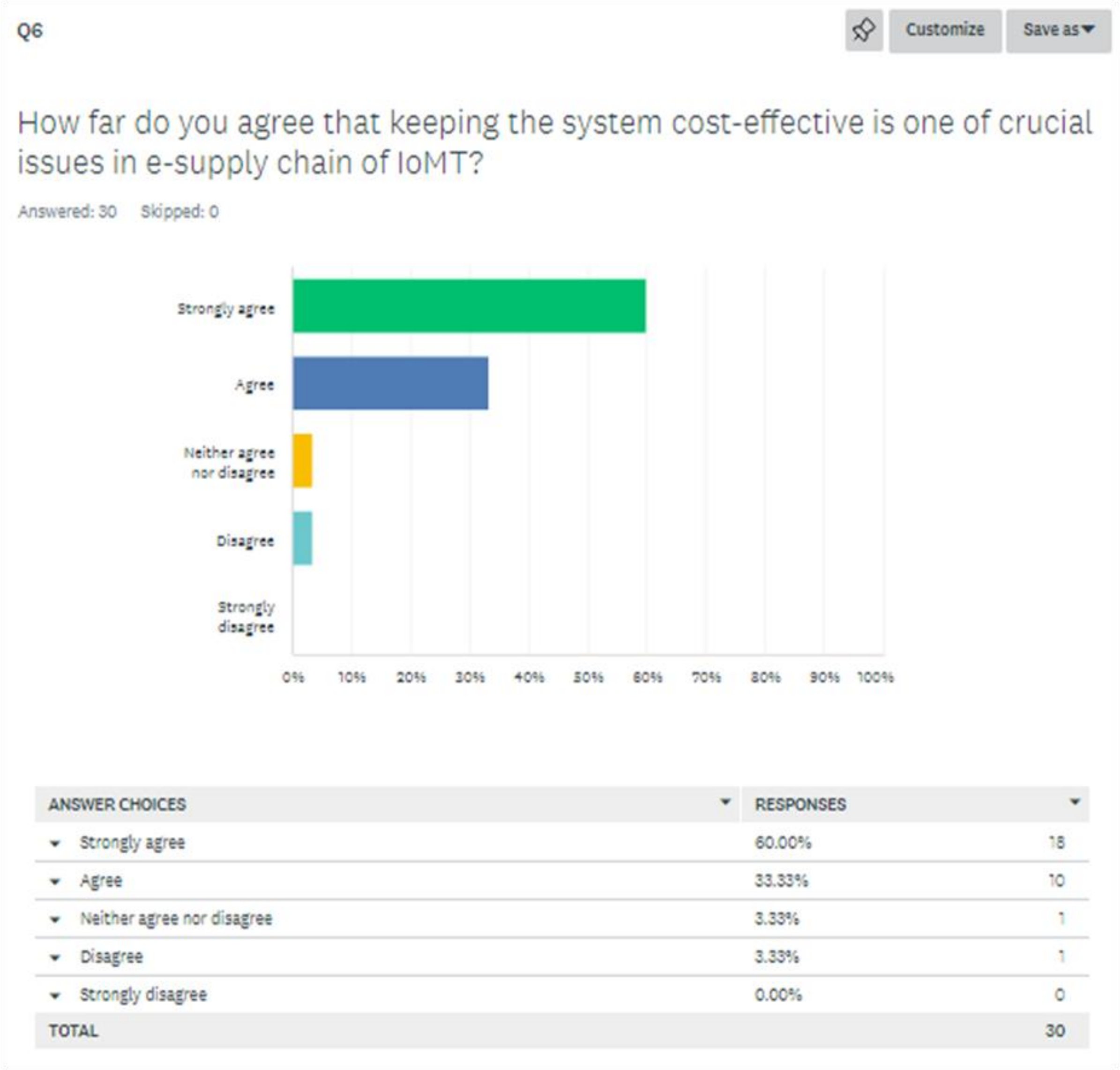
How far do you agree that it can cause negative impact in the entire process?

Answered: 30 Skipped: 0

ANSWER CHOICES	RESPONSES	
Strongly agree	46.67%	14
Agree	46.67%	14
Neither agree nor disagree	3.33%	1
Disagree	3.33%	1
Strongly disagree	0.00%	0
TOTAL		30

In this question, it is being seen that most people strongly agree and agree with the matter that failing to meet customers' expectations will leave a bad impact on the entire process.

6: How far do you agree that keeping the system cost-effective is one of the crucial issues in the e-supply chain of IoMT?



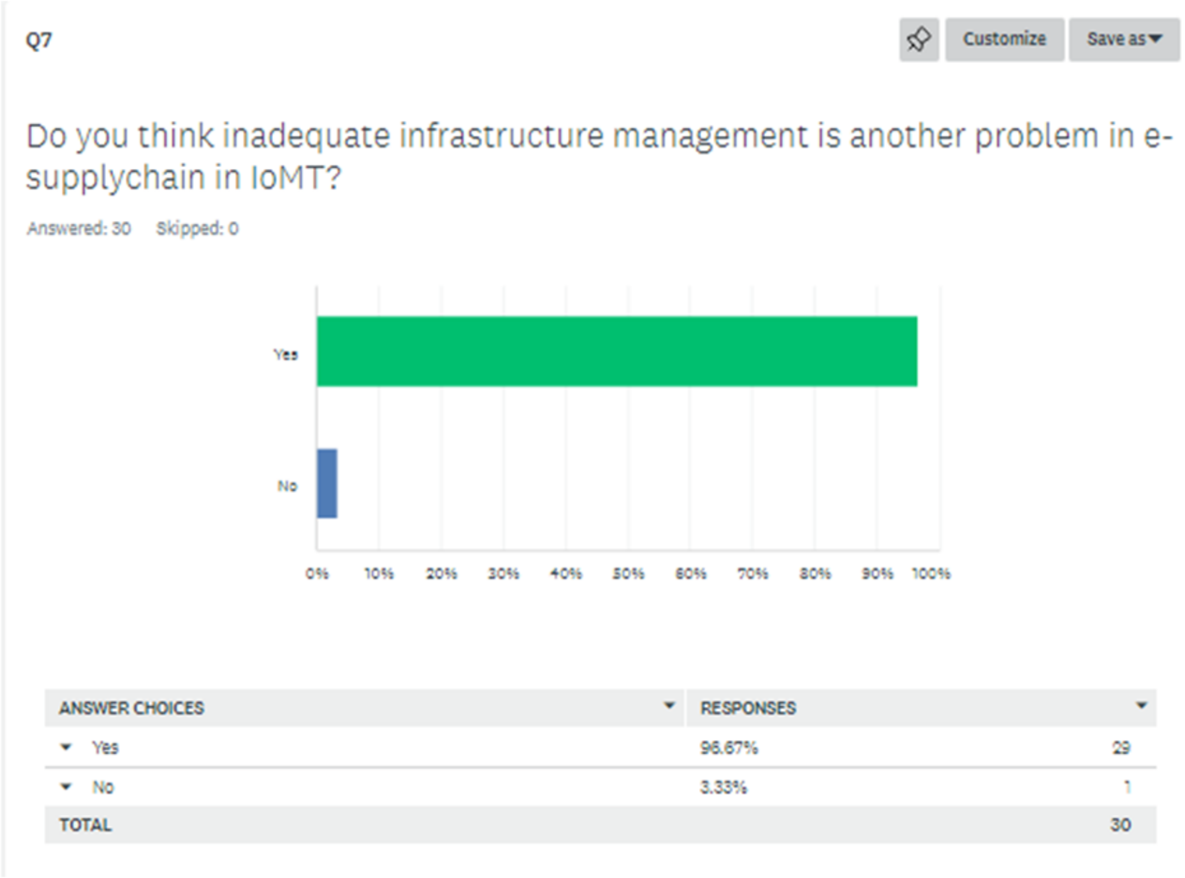
How far do you agree that keeping the system cost-effective is one of crucial issues in e-supply chain of IoMT?

Answered: 30 Skipped: 0

ANSWER CHOICES	RESPONSES	
Strongly agree	60.00%	18
Agree	33.33%	10
Neither agree nor disagree	3.33%	1
Disagree	3.33%	1
Strongly disagree	0.00%	0
TOTAL		30

Sixty per cent of the people strongly agreed with the matter that cost-effectiveness is the crucial issue in the e-supply chain in the IoMT.

7: Do you think inadequate infrastructure management is another problem in e-supply chain in IoMT?



Q7

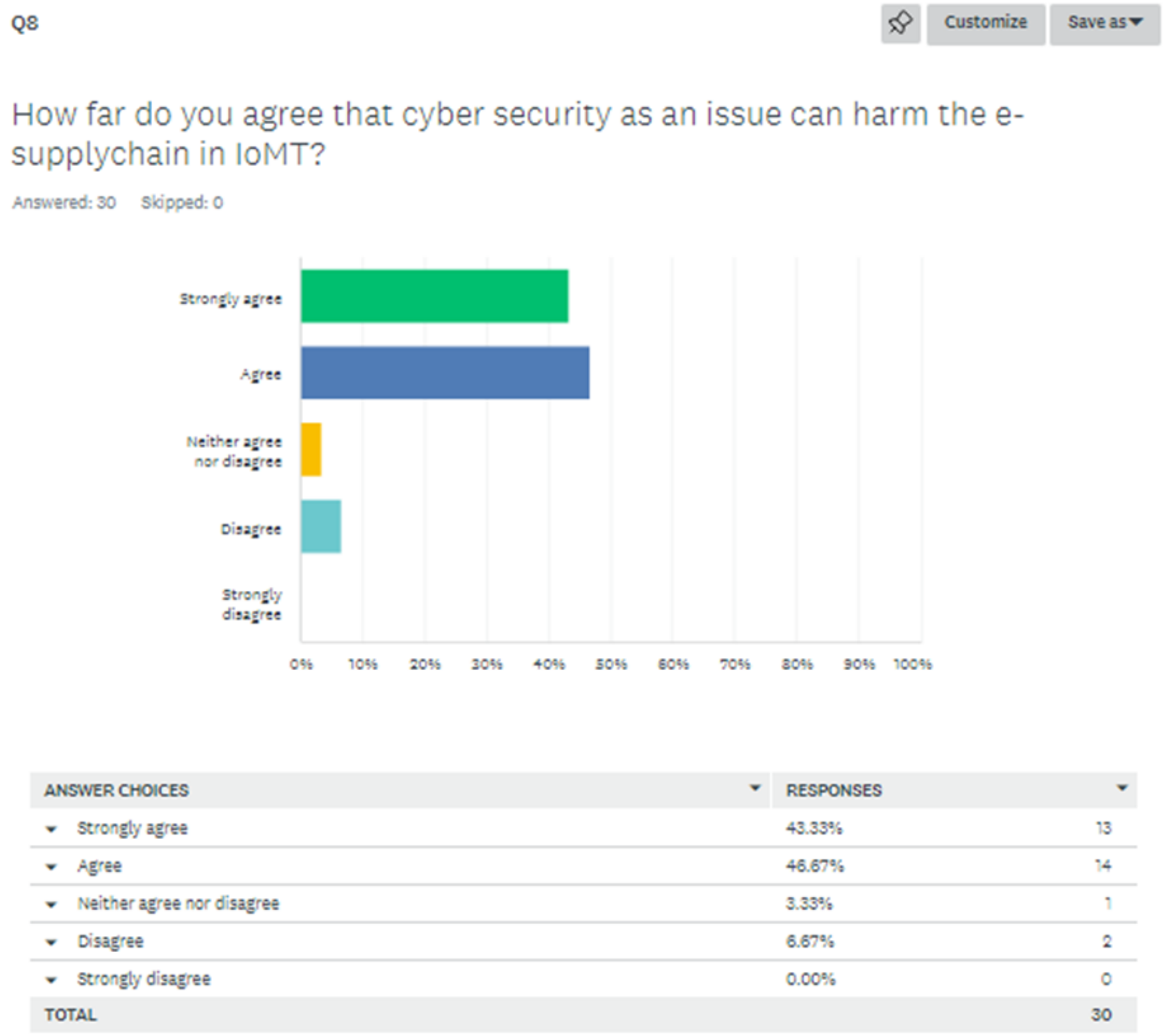
Do you think inadequate infrastructure management is another problem in e-supplychain in IoMT?

Answered: 30 Skipped: 0

ANSWER CHOICES	RESPONSES	
Yes	96.67%	29
No	3.33%	1
TOTAL		30

Inadequate infrastructure is very significant for the e-supply chain management. Most of the respondents have expressed positive reaction to this.

8: How far do you agree that cyber security as an issue can harm the e-supply chain in IoMT?



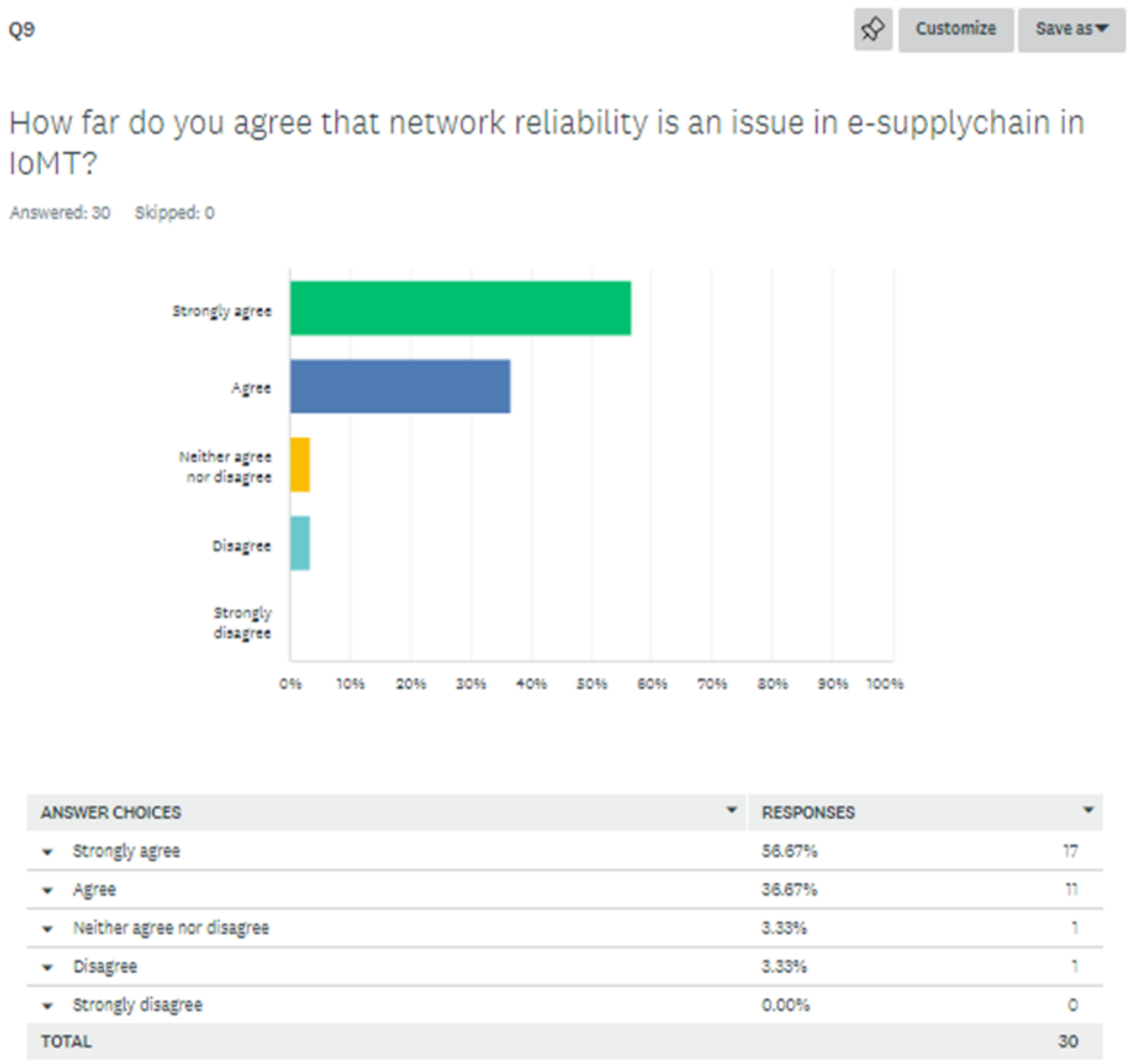
How far do you agree that cyber security as an issue can harm the e-supplychain in IoMT?

Answered: 30 Skipped: 0

ANSWER CHOICES	RESPONSES	
Strongly agree	43.33%	13
Agree	46.67%	14
Neither agree nor disagree	3.33%	1
Disagree	6.67%	2
Strongly disagree	0.00%	0
TOTAL		30

Here in the survey, most of the respondents have stated that they are agreed that cyber security is a major issue, and it can harm the e-supply chain in IoMT.

9: How far do you agree that network reliability is an issue in the e-supply chain in IoMT?



Q9

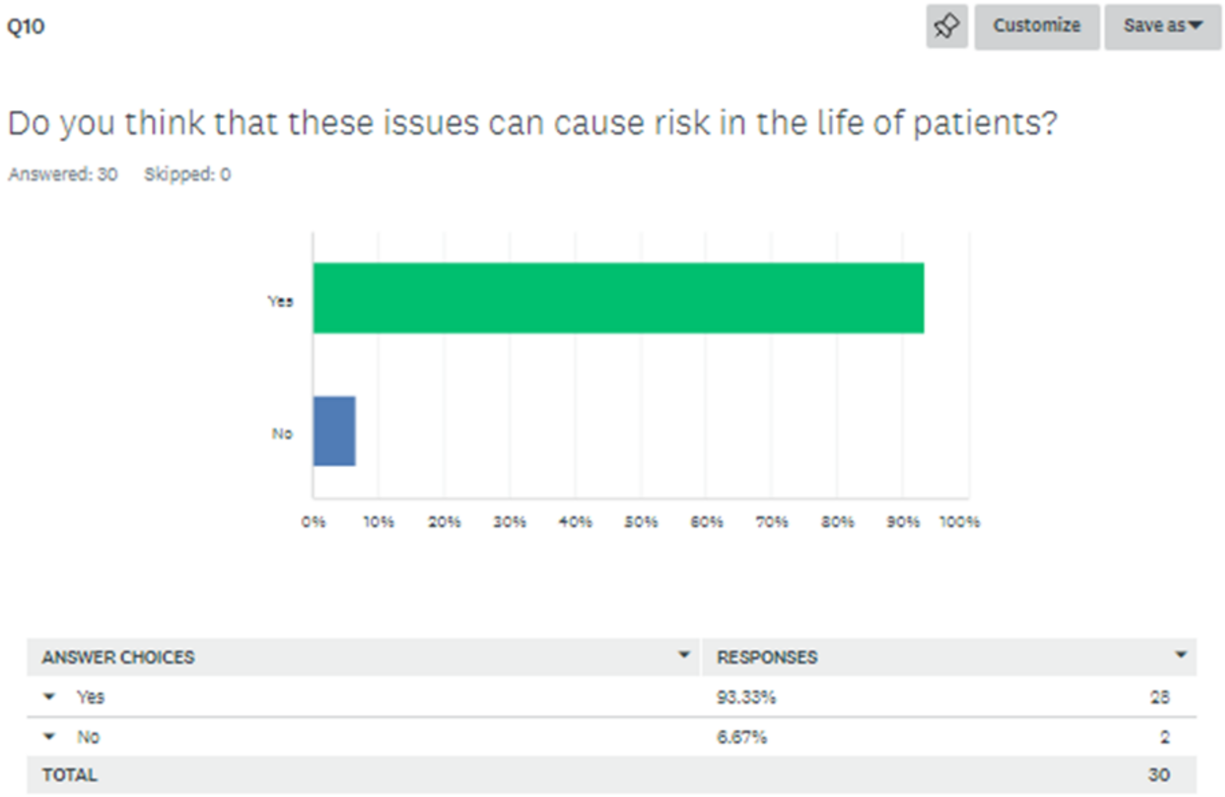
How far do you agree that network reliability is an issue in e-supplychain in IoMT?

Answered: 30 Skipped: 0

ANSWER CHOICES	RESPONSES	
Strongly agree	56.67%	17
Agree	36.67%	11
Neither agree nor disagree	3.33%	1
Disagree	3.33%	1
Strongly disagree	0.00%	0
TOTAL		30

Network reliability is considered as the major issue in the e-supply chain for IoMT as 56 per cent of people strongly agreed with the matter.

10: Do you think that these issues can cause risk in the life of patients?



Q10

Do you think that these issues can cause risk in the life of patients?

Answered: 30 Skipped: 0

ANSWER CHOICES	RESPONSES	
Yes	93.33%	28
No	6.67%	2
TOTAL		30

Out of this, it is understood that most of the respondents are aware that it can cause a serious risk in the life of the patients.

4.2 Statistical Analysis (SPSS)

4.2.1 Descriptive Statistics

The mainly purpose of descriptive analysis assisted to evaluate the survey results that shows multiple results for each question asked by the respondents. Descriptive statistics results summary is given in table 1.

Table 1:

Descriptive Statistics			
	Mean	**Std. Deviation**	**N**
How far do you agree that e-supply-chain in IoMT has various issues?	1.5517	.57235	29
1: What is your gender?	1.2069	.41225	29
what is your age group?	1.6897	.66027	29
Do you think that the e-supply chain in IoMT has a problem in matching the expectation of the patients?	1.1379	.35093	29
How far do you agree that it can cause a negative impact in the entire process?	1.6207	.72771	29

How far do you agree that keeping the system cost-effective is one of the crucial issues in the e-supply chain of IoMT?	1.4828	.73779	29
Do you think inadequate infrastructure management is another problem in e-supply chain in IoMT?	1.0345	.18570	29
How far do you agree that cyber security as an issue can harm the e-supply chain in IoMT?	1.7241	.84077	29
How far do you agree that network reliability is an issue in e-supply chain in IoMT?	1.5172	.73779	29
Do you think that these issues can cause risk in the life of patients?	1.0690	.25788	29

4.2.2 Regression Analysis

To evaluate the significance and construct relationship and dependability of each construct of the research a regression analysis helps to identify the dependability and agreeableness to a question. Table 2 is summarized with regression analysis results.

Table 2:

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.953[a]	.908	.864	.21120

ANOVA						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	8.325	9	.925	20.737	.000[b]
	Residual	.848	19	.045		
	Total	9.172	28			

Out of this ANOVA, the significant value shows the hypothesis significance level that support our research hypothesis and also valid for the survey questionnaire asked by the respondents. Thus, it is understood that all the variables are strongly correlated and highly dependable to each other.

4.2.3. Regression Coefficients

Table 3:

4.2.3. Regression Coefficients

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
	(Constant)	.346	.365		.949	.354
	1: What is your gender?	-.239	.158	-.172	-1.514	.147
	what is your age group?	.312	.105	.360	2.965	.008
	Do you think that the e-supply chain in IoMT has a problem in matching the expectation of the patients?	-.152	.181	-.093	-.843	.410
	How far do you agree that it can cause a negative impact in the entire process?	.539	.146	.685	3.694	.002
	How far do you agree that keeping the system cost-effective is one of the crucial issues in the e-supply chain of IoMT?	-.135	.115	-.173	-1.173	.255
	Do you think inadequate infrastructure management is another problem in e-supply chain in IoMT?	.337	.310	.109	1.088	.290

	How far do you agree that cyber security as an issue can harm the e-supply chain in IoMT?	.126	.098	.185	1.285	.214
	How far do you agree that network reliability is an issue in e-supply chain in IoMT?	-.031	.127	-.040	-.242	.811
	Do you think that these issues can cause risk in the life of patients?	-.050	.289	-.023	-.174	.864

4.2.3 Overall Statistics

Table 4:

Group Statistics					
	How far do you agree that e-supply-chain in IoMT has various issues?	**N**	**Mean**	**Std. Deviation**	**Std. Error Mean**
Do you think that the e-supply chain in IoMT has a problem in matching the expectation of the patients?	Strongly agree	14	1.1429	.36314	.09705
	Agree	15	1.1333	.35187	.09085
How far do you agree that it can cause a negative impact in the entire process?	Strongly agree	14	1.0000	.00000	.00000
	Agree	15	2.1333	.51640	.13333
How far do you agree that keeping the system cost-effective is one of the crucial issues in the e-supply chain of IoMT?	Strongly agree	14	1.0714	.26726	.07143
	Agree	15	1.9333	.79881	.20625
Do you think inadequate infrastructure management is another problem in e-supply chain in IoMT?	Strongly agree	14	1.0714	.26726	.07143
	Agree	15	1.0000	.00000	.00000
How far do you agree that cyber security as an issue can harm the e-supply chain in IoMT?	Strongly agree	14	1.2143	.80178	.21429
	Agree	15	2.2000	.56061	.14475
How far do you agree that network reliability is an issue in e-supply chain in IoMT?	Strongly agree	14	1.0000	.00000	.00000
	Agree	15	2.0000	.75593	.19518
Do you think that these issues can cause risk in the life of patients?	Strongly agree	14	1.0000	.00000	.00000
	Agree	15	1.1333	.35187	.09085

Independent Samples Test										
		Levene's Test for Equality of Variances		**t-test for Equality of Means**						
			Sig.		**f**	**Sig. (2-tailed)**	**Mean Difference**	**Std. Error Difference**	**95% Confidence Interval of the Difference**	
									Lower	**Upper**
Do you think that the e-supply chain in IoMT has a problem in matching the expectation of the patients?	Equal variances assumed	021	887	072	7	943	. 00952	. 13279	-.26294	.28199
	Equal variances not assumed			072	6.716	943	. 00952	. 13294	-.26338	.28243
How far do you agree that it can cause a negative impact in the entire process?	Equal variances assumed	.319	047	8.202	7	000	-1.1333	.13818	1.41686	-.84980
	Equal variances not assumed			8.500	4.000	000	-1.1333	.13333	-1.4193	-.84736

How far do you agree that keeping the system cost-effective is one of the crucial issues in the e-supply chain of IoMT?	Equal variances assumed	.419	.045	3.838	27	.001	-.86190	.22459	-1.3227	-.40109
	Equal variances not assumed			3.949	7.292	001	-.86190	.21827	-1.3218	-.40199
Do you think inadequate infrastructure management is another problem in e-supply chain in IoMT?	Equal variances assumed	.043	033	.036	7	309	.07143	.06892	-.06997	.21283
	Equal variances not assumed			.000	3.000	336	.07143	.07143	-.08288	.22574
How far do you agree that cyber security as an issue can harm the e-supply chain in IoMT?	Equal variances assumed	059	810	3.859	7	001	-.98571	.25544	-1.5098	-.46160
	Equal variances not assumed			3.812	3.104	001	-.98571	.25859	-1.5205	-.45091
How far do you agree that network reliability is an issue in e-supply chain in IoMT?	Equal variances assumed	.586	026	4.944	7	000	-1.0000	.20228	-1.4150	-.58496

	Equal variances not assumed			5.123	4.000	000	-1.0000	.19518	-1.4186	-.58138
Do you think that these issues can cause risk in the life of patients?	Equal variances assumed	1.203	002	1.416	7	168	-.13333	.09416	-.32653	.05986
	Equal variances not assumed			1.468	4.000	164	-.13333	.09085	-.32819	.06152

Out of this, it is found that most of the sig (2 tailed) values are higher than 0.5 can be summarized as significant and accepted to this research, it can be understood that all the hypotheses are valid and supported in current analysis.

5. DISCUSSION

The development of interconnected medical devices have transformed the fundamentals of healthcare operations owing to trying to cut technological developments. As both a result, data security for medical equipment has received much interest. The health care industry will experience a total change in terms of the adaptation of innovative communication technology, including such 5G networks. They shall have seen a new paradigm in the healthcare sector as a result of the rapid advancement of communications technology. Miscommunication problems, modern, trying to cut healthcare frameworks will be unable to perform telesurgery. Ambulance crews will indeed be superseded by 5G, and new tech will be reinvented. Furthermore, since of improved technology, this platform is exposed to various security flaws, which might present a serious risk to the security and privacy of patients. As both a consequence, current safety issues have prompted researchers to investigate various medical device vulnerabilities. Furthermore, proper control methods which can preserve the integrity and security of IoMT systems is crucial since security is a critical component of ensuring the dependability of IoMT devices and for the successful implementation of this technology into medical systems.

6. CONCLUSION AND FUTURE RECOMMENDATIONS

In conclusion, it can be claimed that the e-supply chain in the IoMT is overwhelmed by a number of problems. Meeting consumer expectations, inadequate infrastructure, cost-effectiveness, cyber security, and network dependability are some causes of these problems. The service provider of the IoMT's e-supply chain may find some of the solutions provided in this research that can have ultimate impact on healthcare strategic management and other managerial areas.

Future research might focus on the question of how the solution could be implemented in the IoMT more successfully, the roles of the medical personnel in relation to the problems, and how the workers at the ground level could be trained in this area to effectively reduce the likelihood of cybercrime.

REFERENCE

[1] 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.

[2] 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.

[3] 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.

[4] G. Kanagavalli and R. Azeez, "Logistics and E- Logistics Management: Benefits and Challenges," *Int. J. Recent Technol. Eng.*, vol. 8, no. 4, pp. 12804–12809, 2019, doi: 10.35940/ijrte.d7179.118419.

[5] 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.

[6] A. Yeboah-Ofori *et al.*, "Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security," *IEEE Access*, vol. 9, no. Ml, pp. 94318–94337, 2021, doi: 10.1109/ACCESS.2021.3087109.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[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] F. Ma, T. Sun, L. Liu, and H. Jing, "Detection and diagnosis of chronic kidney disease using deep learning-based heterogeneous modified artificial neural network," *Futur. Gener. Comput. Syst.*, vol. 111, pp. 17–26, Oct. 2020, doi: 10.1016/j.future.2020.04.036.

[13] 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.

[14] 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.

[15] 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.

[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] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] S. S. Aljameel, I. U. Khan, N. Aslam, M. Aljabri, and E. S. Alsulmi, "Machine Learning-Based Model to Predict the Disease Severity and Outcome in COVID-19 Patients," *Sci. Program.*, vol. 2021, 2021, doi: 10.1155/2021/5587188.

[29] 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.

[30] 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.

[31] 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.

[32] A. Garcia-Perez, J. G. Cegarra-Navarro, M. P. Sallos, E. Martinez-Caro, and A. Chinnaswamy, "Resilience in healthcare systems: Cyber security and digital transformation," *Technovation*, no. August 2021, p. 102583, 2022, doi: 10.1016/j.technovation.2022.102583.

[33] 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.

[34] 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.

[35] 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.

[36] A. Hussain, R. Wenbi, A. L. Da Silva, M. Nadher, and M. Mudhish, "Health and emergency-care platform for the elderly and disabled people in the Smart City," *J. Syst. Softw.*, vol. 110, pp. 253–263, 2015, doi: 10.1016/j.jss.2015.08.041.

[37] 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.

[38] G. M. Qasaimeh and H. E. Jaradeh, "THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE EFFECTIVE APPLYING OF CYBER GOVERNANCE IN JORDANIAN COMMERCIAL BANKS," *Int. J. Technol. Innov. Manag.*, vol. 2, no. 1, 2022.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] J. Almalki *et al.*, “Enabling Blockchain with IoMT Devices for Healthcare,” *Information*, vol. 13, no. 10, p. 448, 2022, doi: 10.3390/info13100448.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] M. Asif, S. Abbas, M. A. Khan, A. Fatima, M. A. Khan, and S. W. Lee, “MapReduce based intelligent model for intrusion detection using machine learning technique,” *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2021, doi: 10.1016/j.jksuci.2021.12.008.

[53] 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.

[54] 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.

[55] S. Lancaster, D. C. Yen, and C. Y. Ku, “E-supply chain management: An evaluation of current web initiatives,” *Inf. Manag. Comput. Secur.*, vol. 14, no. 2, pp. 167–184, 2006, doi: 10.1108/09685220610678613.

[56] 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.

A SYSTEMATIC REVIEW OF BLOCKCHAIN TECHNOLOGY USE IN E-SUPPLY CHAIN IN INTERNET OF MEDICAL THINGS (IOMT)

Romil Rawat

University of Extremadura, Spain

rawat.romil@gmail.com

ABSTRACT

For every sector, managing supply chains is a difficult task, but the healthcare sector faces risks and complication since a disrupted supply chain could have a direct impact on patient security and medical results. In this assignment we will discuss how Blockchain technology is one possible method for enhancing the health E-supply chain's security, integrity, data provenance, and usefulness. The medical supply, medical product and supply, Internet of Medical Things (IOMT), and health care sector are all given such priority, the goal of this research is to provide a description of the advantages and drawbacks of using blockchain technology in the medical distribution and supply network. The unfulfilled potential of blockchain technology to increase the health supply chain requires greater research, analysis, and integration with regulatory frameworks has been discussed.

Keywords: E-Supply Chain, Blockchain, IoMT.

1. INTRODUCTION

Globalization, increasing usage of information systems and related technology, and a sector populated by various businesses in several jurisdictions have all contributed to the development of a complex and self-replicating health supply chain. One of several initiatives to safeguard supply chains in the broader sense of all commodities and items is the US National Strategy for Global Supply Chain Security. "Promote efficient and secure services" and "increase resilience" are two

Online: https:// doi.org/10.54489/ijcim.v2i2.119 Publisher: **GAF-TIM**, https://gaftim.com

goals of the White House [1]. Although this government plan for SC security is crucial for all industries, the healthcare sector is particularly in need of it since a compromised supply chain can have several negative effects on resulting health and patient safety. These include chance of failure to store and deliver life-saving supplies, unfavorable outcomes related to supply chain breaches, and a rise in end-user or patient morbidity and death [2].

When creating technology-driven solutions and use cases, one of the verticals that is most heavily considered is the pharmaceutical supply chain [3]. For instance, billions are spent annually on the worldwide market for subpar, counterfeit, and grey market medications. Studies have indicated that many medications, medical equipment, and biologics are counterfeited in low-, middle-, and high-income countries. This shows that this kind of global pharmaceutical criminality affects the entire drug supply chain. Supply chain vulnerabilities as well as new types of technologies have emerged as a result of the introduction of digital health platforms, along with the expansion of the pharmaceutical business internationally and an increase in worldwide medication sales [4]. Up until now, Technology like ownership-transferable radio frequency identification (RFID) chips, smartphone apps to trace pharmaceutical pedigree (for example m-pedigree), and other item authentication systems have received the majority of the attention in efforts to protect and improve supply chain [5].

Enhancing security and reducing risks in the space available of healthcare goods and equipment is a priority issue in relation to pharmaceutical counterfeiting. Given the growth of linked devices and mobile health (mHealth) applications, the medical device business is particularly significant. Examples of difficulties with the expansion of the Internet of Medical Things (IOMT) and how its advancement and acceptance have greatly surpassed security needs include people with implanted cardiac devices being made susceptible owing to massive security gaps [6]. Governmental organizations and authorities are taking action to raise public responsiveness of the hazards to the public and the healthcare network in the IOMT in response to problems like the cybersecurity vulnerability found in pacemakers. Put another way, escalating medical supply prices are prompting healthcare organizations to reevaluate fundamental operational tenets [7]. Even though these procedures would enable systems to make greater use of a health system setting with abundant distribution network information, supply management still wouldn't be entirely facilitated.

1.1 Problem definition

The penetration of the mutual classification of substandard and falsified (SF) medications is a severe and well-known hazard to the pharmaceutical supply chain, which are typically stated as fake items. However, it usually take on an unique authorized meaning. These several forms of tainted and fake pharmaceuticals may show up as a result of drug theft and diversion, poor manufacturing practices or improper storage, importation of subpar medications without local authorization, and entry of subpar or fake items into grey markets [8]. Would blockchain technology be a better supply chain and anti-counterfeiting system than the ones we currently have? These are the key inquiries to ask in order to fully comprehend how blockchain can protect and enhance supply chain activities for the creation, dissemination, and distribution of medical products [9]. Does it have features or processes that aren't present in legacy systems or centralized databases? What kind of interactions might a blockchain have with pre-existing supply chain data like RFID, GS-1, EPCIS, and anti-counterfeiting technology? Can it provide a regulatory and compliance solution that can reduce risk while also boosting compliance and patient safety, hence enhancing both manufacturer and customer benefits?

1.2 Proposed Solution

Crisis and disaster mitigation and management, including shielded goods for medical personnel access to vital drugs, vaccinations, and immunizations during public health emergencies, as well as essential medication, vaccine, and access issues, are all aspects of the public health supply chain that need to be addressed [10]. Blockchain technology use case scenarios in the healthcare supply chain and combating SF medicines of ensuring access to necessary and superior medicines all interact with use case scenarios for sustaining satisfactory stock at point of sales (e.g., qualifying stock outs) [11], speeding up the effective delivery of health services and supplies, and reducing corruption in the health systems' drug procurement processes [12].

One way to address the issues is through the deployment of blockchain technologies for things like product tracing, verification, detection, and notification as well as source data. Following are some of these problems and their solutions: -

- Product identification - The use of block chains is consistent with the requirement for a unique product identity that is validated as a side chain [13].

- Product Tracing -With the help of product tracing, producers, distributors, and dispensers may supply tracing data in a common ledger with automated confirmation of crucial data.
- Product Verification- Product identification and other supplied information are verified using an open system that is created for this purpose [14].
- Detection & Response - Enables both public and private actors to report and discover medications that may be hazardous, illegal, or counterfeit [15].

Public health supply chain difficulties involve tragedy and crisis management and handling, including availability to necessary drugs, vaccinations, and immunizations, as well as protective materials for healthcare personnel during public health emergencies [16]. In order to guarantee access to required and high-quality medications, blockchain technology applications intersect with use cases in the healthcare supply chain and fight SF drugs[17]. These applications include maintaining sufficient quantities at the distribution point (e.g., preventing stock outs) [18], decreasing the corruption associated with health systems in the purchase of pharmaceuticals, and speeding up the effective provision of healthcare and commodities. [19].

In order to establish strong use cases and localize the context of the myriad experiments encountered by supply chains in different countries [20], the answers to these questions should serve as the basis for first evaluation of blockchain design features and feasibility studies [21]. Using the Drug Supply Chain Security Act (DSCSA) as an example, each regulatory element must be compatible with bitcoin technology for anything to be a workable solution. By creating use scenarios, simulation studies, and blockchain solution prototypes, a number of enterprises are dynamically investigating the presentation of blockchain for medicinal supply chain [22]. The thought process behind this research is being led by the Center for Supply Chain Studies, a nonprofit organisation established to investigate the practicality of innovation through a virtual pilot project with participation from many stakeholders from throughout the pharmaceutical supply chain [23]. Furthermore, it is working on reference models for DSCSA and blockchain scalability and compatibility.

In order to investigate technical professional organizations have also planned workshops, webinars, and are currently overseeing a Supply Chain/Clinical Trials Technology Implementation Industry Connections program [24]. These initiatives aim to improve patient safety in both the pharmaceutical supply and clinical trials sectors. Several businesses are concurrently pursuing these objectives from various angles [25]. For example, they are developing use cases, looking into vendor partnerships [26], and incorporating blockchain technology into pharmaceutical and related healthcare applications, as well as other industries (such food supply chains) [27].

A case study reviewed has been looking at how blockchain technology might increase the security of the pharmaceutical supply chain while at the same time mentioning the combating long-lasting clinical experiment of SF medications [28]. Several players in the blockchain research and startup communities for advances, public health, and healthcare have expressed interest in this case study [29]. Even though a study like MediLedger shows a cooperative approach across multiple groups, the concrete and practical application of blockchain to this issue is still uncertain and requires additional work.

Private blockchains are beginning to emerge in other healthcare specializations that are usually tech-focused and subject to tight regulation, outside of pharmaceutical and the medicinal distribution chain [30]. Clinical trial participants, health information and data processing providers and businesses, and as previously said, the medication supply chain are perhaps the most developed healthcare industries going forward with blockchain implementation [31]. However, there are applications for medical equipment and supply, IOMT, and public health that are aligned with the core concepts of better data management [32] and the reliability of the wellness supply chain, and these are briefly discussed below [33].

Medical equipment and supplies for a security weakness that exposed the device to possible hacker operation, over half a million customers with implanted cardiac pacemakers were recently recognized as requiring a crucial firmware upgrade [34], [35]. This comes after past incidents, such as the SymbiqTM Infusion System recall, when it was found that Hospira's smart pumps could well be retrieved and operated by unauthorized users over a hospital network to adjust patients' doses [36]. The appropriate usage of these technologies along with their risks become increasingly obvious as the use of linked and digitally enabled medical equipment increases [37].

Additionally, due to its efficiency and accountability around trust, blockchain does have potential to save costs, In response to the FDA and EU legislation requiring that medical equipment possess a Unique Device Identifier (UDI) enhance patient safety and prevent medical device fraud [38]. Blockchain technology has the potential to enhance equipment preventative maintenance through the use of automated smart contracts [39], [40]. The National Health Service (NHS) National Services Scotland, Edinburgh Napier University, and Spiritus Development are working together in a university-industry partnership using blockchain technology to help the medical equipment supply chain and track devices throughout their lives, with assistance from The Data Lab and Scottish Funding Council. The pilot's secondary goal is to observe the opportunities used in patient care to use analytics to increase efficiency and security, such as quicker responses to instrument recalls and field alerts from responsible businesses and authorities [41].

By enhancing logistics operations and connecting clinical communities, blockchain technology also has the potential to lower costs and increase the value of healthcare. In order to do this, Johns Hopkins Medicine (JHM) established a supply chain strategy with an emphasis on managing blood, joints, and the spine [42]. JHM placed this cost effective program with a "things not staff" mentality to focus on lowering supplier expenses rather than employee cutbacks while maintaining a focus on increasing the value of treatment. One of the most well-known outcomes of this JHM program was the Armstrong Institute for Patient Safety and Quality (AIPSQ), and it was noted that the coordination of these interrelated initiatives was a crucial factor in its success [40].

With their healthcare medical societies concentrating on supply management of medical goods, the communities for spine, joint, and blood management collectively contributed to realizing millions in cost reductions. When considering how blockchain technology might secure and optimize SCM for the production, delivery [43]. The first thing that should be considered is whether or not it would be a better alternative to the logistical network, anti-counterfeiting systems, and databanks [44]. The need to recognize whether it have functions or procedures that aren't found in centralized databases or legacy systems? What potential interactions could a blockchain have with prevailing supply chain data like RFID, Global Standards One (GS-), Electronic Product Code Information Services (EPCIS), and anti-counterfeiting technology? Can it provide a regulatory and compliance solution that can reduce risk while also boosting agreement and patient security and safety by enhancing both manufacturer and customer benefits?

2. LITERATURE REVIEW

Recently, over 500,000 patients with implanted cardiac pacemakers were recognized as requiring a critical firmware upgrade owing to a potential weakness that exposed their implant to potential hacking [45]. This follows earlier incidents, such as the removal of the SymbiqTM Infusion System [46] when it was revealed that unauthorized individuals could access and manipulate Hospira's smart pumps over a hospital network to adjust patients' doses [47], [48]. As the usage of linked and digitally enabled medical equipment grows in popularity, so do their appropriate applications and risks [49].

The use of blockchain might help improve preventative maintenance of equipment through the implementation of smart contracts [50]. Recently, over 500,000 patients with implanted cardiac innovators were recognized as requiring a critical firmware upgrade owing to a security weakness that exposed their device to potential hacking [51]. This follows earlier incidents, such as the recall of the SymbiqTM Infusion System when it was revealed that unauthorized individuals could access and manipulate Hospira's smart pumps over a hospital network to adjust patients' doses [52].

As the usage of linked and digitalized medical equipment grows in popularity, so do their appropriate applications and vulnerabilities [53], [54]. The use of blockchain might help improve device preventative maintenance by deploying a medical products supply network to track devices throughout their lives [45]. The pilot will also look for ways to use analytics to improve quality and reliability throughout the patient care route [55]. For example, Farma Trust is creating a blockchain solution for the pharmaceutical supply chain, as well as an Initial Coin Offering (ICO) particularly for the European market [56]. A corporation like Walton is in the early stages of using RFID and IoT; with the purpose of scaling to the business ecosystem, a startup named Chronicled has teamed with The LinkLab for a blockchain-enabled DSCSA compliance platform.

3. RESEARCH METHODOLOGY

This research aims to assess prior work that applies blockchain technology to the healthcare sector. The shortlisted papers were grouped using research questions. In order to conduct systematic review a secondary study that first establishes clear research objectives before gathering, organizing, and extracting all available material to address those concerns. There are several writing guides available for systematic literature reviews. To perform the current research, nevertheless, Barbara Kitchenham's suggestions are followed. Review papers published in journals with high impact factors adhere to this practice. This method was developed expressly for carrying out systematic literature review for proposed research.

In order to identify the technology's greatest potentials in the healthcare industry, this research concentrated on elaborating on its qualities. To totally reform the system, it is also necessary to explore the uses of blockchain technology in-depth with all the stakeholders in the healthcare industry. Furthermore, this review of the literature follows a specific set of steps to obtain findings that set it apart from earlier non-structured reviews.

4. DATA ANALYSIS

The findings of this study are created in response to the first stage of the systematic literature review to fill in the gaps identified, as indicated below.

Motivating the research question

Q.1 What are the main concerns of the stakeholders in healthcare?

The goal is to draw attention to the significant problems impeding the healthcare sector's performance.

Q.2 What Blockchain functionalities are applied to address the concerns found?

The goal is to investigate cutting-edge technology that advances the relevant concerns and the industry.

Q.3 What are the difficulties and problems in implementing blockchain technology?

The objective is to identify any unresolved implementation concerns using blockchain technology.

In order to find as much material as possible, numerous studies were gathered after rigorous examination of various databases and publications. Throughout this stage, it was discovered that certain papers were fully or partially out of relevance, while others were determined to be precisely connected with the study field (Blockchain and Healthcare). Given their titles and cited keywords were determined to be comparable to popular search, inclusion criteria reduced the studies to a few. Studies from renowned publishers and publications with high impact factors were selected. Prior to categorizing the studies, we first evaluated each study's abstract considering the publications' research topics, methodologies, and conclusions. The additional searched documents were disregarded since their titles and abstracts lacked the required keywords. Additionally removed were duplicate or pointless research and articles written in languages other than English.

5. DISCUSSIONS

This section of the assignment provides details on the study questions listed in the Methodology and further divided into subsections. The subsections include lists of the aspects of the blockchain that can address the issues the healthcare industry is currently experiencing, a breakdown of the common problems in that sector by the numerous participants, and finally research that highlights the issues and challenges with blockchain implementation that would need to be resolved in the future. The Discussions of the assignment are based on the below questions which are precisely answered.

5.1 Q.1 What are the principal concerns involving Healthcare Stakeholders?

Ans: -A system is made up of a number of components or items that interact to produce a useful result. Providers, patients, payers, supply chain bearers (manufacturers, suppliers, pharmacies), and research organizations are the five key participants that make up the healthcare sector. A significant component and typical third party are the provider (hospital, doctor, specialist, etc.). Some problems that are serious topics of worry are being faced by each player. Under each situation, the following concerns are covered:

- *Providers*

A main participant in the healthcare industry is a provider. For doctors and patients to have excellent results, patient information management is crucial. The management and curation of the patient records, however, presents various difficulties. Additional time and resource costs may result from a lack of interoperability standards for sharing patient records among labs and hospitals. For patients, payers, and pharmacies, providers serve as a reliable third party.

- *Patients*

The most significant component of the health sector is the patient. Although providers collect patient health information, patients do not have the legal authority to grant or deny access to medical information as they see fit.

- *Payers*

Insured claim payments made by payers (insurer or employer) on behalf of patients must also be validated from centric IT systems, which are prone to security flaws and deliberate fraud. Records (bills, prescriptions, etc.) can be fabricated using phony credentials for medical professionals, incorrect invoicing, false tests, etc. To track legitimate insurance claim procedures, accounting and data provenance are essential.

- *Research Organizations*

To keep track of emerging ailments, develop therapies for them, and find new drugs, research centers and pharmaceutical corporations need public health data. The exchange of health care data is a requirement for clinical audit, national data collecting, and research. Without the patients' consent, a physician may disclose patient data with these groups, which is against patient privacy.

- *Pharmaceutical Supply Chain Management*

The sellers, agents, processors, and pharmacies are the main participants in the pharmaceutical supply chain. It is a complicated system with a wide variety of manufacturing, storage, distribution, and raw material acquisition-related operations. Reliability must be ensured by proper administration and oversight. The origins and quality of drug ingredients may come from a variety of uncertified sources.

5.2 Q.2 What aspects of the blockchain are employed to address the problems found?

The main advantage of blockchain technologies is their adaptability to various situations. By applying the blockchain technology's following capabilities and addressing the industry's key problems, the healthcare sector may progress quickly. The capabilities are addressed and discussed as below: -

- *The problem of record management is solved via Distributed Digital Ledger*

Every firm must maintain its records effectively in order to succeed, and this demands a significant investment in both human and technological resources. Blockchain, a decentralized distributed ledger technology, promises to replace the present expensive systems with less expensive, simpler-to-implement solutions that are more productive and efficient.

- *The problem of data interchange is solved by interoperability*

The inconsistent fragmentation of patient health records may be resolved by blockchain distributed ledger technology, enhancing provider communication and quality. Since the data flow will positively affect market competition, it will promote real-time patient communication, the sharing of the most recent health and treatment information, and quicker product creation.

- *The problem of safety and privacy is solved via consensus mechanisms and cryptography*

Immutable blockchain's capacity to capture consumers' attention by demonstrating accuracy and consistency and transparency is its charm. By utilizing the consensus algorithm and strong encryption in blockchain technology, patient-controlled safe access is ensured because only the private key may decode the data.

- *Lack of data provenance is resolved via traceability and time stamping*

Payers can avoid risky financial loss by using time-stamped, validated records for claim qualifying. Clinical study results must be transparent, free of data eavesdropping, with precise endpoint switching, etc.

- *The monetization problem is solved by digital currency*

In a blockchain-based network, miners receive bitcoin as payment for using their processing power to support and maintain the network.

Now that the healthcare sector has embraced blockchain technology, what issues does it now face?

- Scalability: When a blockchain-powered health care incorporates sensor devices for patient care, storage issues and computationally intensive tasks must be overcome.
- Security (risk of attack of 51%): Consensus powers the blockchain. Malicious miners may control the majority, or more than half, of all nodes, or 51%, and prevent other honest miners from accepting their blocks. Their increased computing

power may also let them to steal valuable data or currencies. A bigger network, however, reduces the likelihood of this attack.

- Confidentiality disclosure: Because the blockchain database is open - source platform, it is subject to the restriction that "openness reveals confidentially." Because patient-related records are so delicate, it is particularly important for patient healthcare records and biomedical applications.
- Confidentiality and identity privacy: The ambiguity and fraud hype that surrounds blockchain is another issue. Criminals may use cryptocurrency while benefiting from the blockchain network's anonymity. On the Dark Web, individuals may use bitcoins to purchase illicit substances.
- Unsustainability for the environment: Another problem with existing blockchain implementations is their inefficiency and unreliability for the environment. The wattage required by the "proof-of-work" requirements in current blockchain implementations is equivalent to powering a single Bitcoin transaction.
-

6. CONCLUSIONS AND FUTURE RECOMMENDATIONS

The potential benefits of blockchain technology are some possible advantages for enhancing supply chain management: 1) eliminating fraud and mistakes; 2) cutting down on paperwork delays; 3) improving stock control; 4) identifying issues faster; 5) lowering parcel expense; and 6) improving/building customer trust. However, applying these latent assistances to urgent supply chain issues in the healthcare industry is still a promise unfulfilled. In the future, more financing and research will be needed. However, applying these potential benefits to urgent supply chain issues in the healthcare industry is still a promise unfulfilled. In the future, more research and funding may be needed to boost supply chain performance.

As evidenced by the requirement to adhere to legal frameworks like the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union, it is equally challenging to identify confidentiality and privacy concerns specific to the healthcare sector. Although many blockchain-based health supply chain initiatives are still in the Proof of Concept (PoC) or pilot stage, more mature installations are being looked into across other industrial sectors that can be implemented for the healthcare sector and centralised to policy rewards provided by governments (e.g., compatibility with the DSCSA). The health supply blockchain appears to have endless potential and opportunities.however only time will prove if the highly regulated and complicated healthcare sector can fully exploit everything that blockchain technology has to offer.

The use of blockchain technology in IOMT computation and medical healthcare is also very young. With its characteristics and qualities, this technology offers significant potential to address some of the most pressing problems in the E-supply chain of the healthcare industry. The ecology might undergo a technological revolution. However, a significant amount of research must be done on the pharmaceutical supply chains and health insurance systems. It is essential to manage the health E-supply chain well in order to guarantee the best patient safety and outcomes for overall community health. Paradoxically, this activity depends on cutting-edge innovation but does not properly utilize it. A medical supply chain with flaws, such as the international trade in counterfeit drugs, stock outs and shortages of medications, and security flaws in connected medical equipment, highlight how high stakes this industry is in comparison to others. As a result, solutions must consider and strike a balance between E-supply chain management optimization, supply chain efficiency, and risk mitigation. Enhancing the health supply chain's functionality, resilience, integrity, and data provenance is crucial across all healthcare verticals.

Future study, financing, and design of systems that can be systematically assessed for their real determinant of patient safety and public health outcomes will be necessary. There will probably also be a lot of use scenarios in the healthcare industry. Medication recall management and combating prescription drug addiction are two other examples from the pharmaceutical industry that highlight special advantages that a blockchain-powered procurement may provide (e.g., opioids).

Another key method through which blockchain technology might aid in improving supply chain performance is the ability to use decentralized applications to automate procedures and cut expenses. It is challenging to manage privacy and data protection issues related to the E-supply chain of the healthcare business, as evidenced by the Health Insurance Portability and Accountability Act necessity to comply with legal frameworks.

REFERENCES

[1] 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.

[2] T. M. Ghazal *et al.*, “Optimization Procedure for Intelligent Internet of Things Applications,” in *2022 International Conference on Business Analytics for Technology and Security, ICBATS 2022*, 2022, pp. 1–6. doi: 10.1109/ICBATS54253.2022.9759065.

[3] 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.

[4] T. M. Ghazal, A. U. Rehman, M. Saleem, M. Ahmad, S. Ahmad, and F. Mehmood, “Intelligent Model to Predict Early Liver Disease using Machine Learning Technique,” in *2022 International Conference on Business Analytics for Technology and Security, ICBATS 2022*, 2022, pp. 1–5. doi: 10.1109/ICBATS54253.2022.9758929.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] T. M. Ghazal *et al.*, “Alzheimer disease detection empowered with transfer learning,” *Comput. Mater. Contin.*, vol. 70, no. 3, pp. 5005–5019, 2022, doi: 10.32604/cmc.2022.020866.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] T. M. Ghazal *et al.*, “IOT for Smart Cities: Machine Learning Approaches in smart healthcare---A Review,” *Futur. Internet*, vol. 13, p. 8, Aug. 2021.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] H. M. Alzoubi, B. Al Kurdi, I. Akour, and M. T. Alshurideh, “The effect of blockchain and smart inventory system on supply chain performance: Empirical evidence from retail industry,” *Uncertain Supply Chain Manag.*, vol. 10, no. 4, pp. 1111–1116, 2022, doi: 10.5267/j.uscm.2022.9.001.

[34] 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.

[35] 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.

[36] 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.

[37] T. M. Ghazal, S. Abbas, M. Ahmad, and S. Aftab, “An IoMT based Ensemble Classification Framework to Predict Treatment Response in Hepatitis C Patients,” in *2022 International Conference on Business Analytics for Technology and Security, ICBATS 2022*, 2022, pp. 1–4. doi: 10.1109/ICBATS54253.2022.9759059.

[38] 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.

[39] 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.

[40] 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.

[41] T. M. Ghazal and N. Taleb, *Feature optimization and identification of ovarian cancer using internet of medical things*. Expert Systems, 2022. doi: 10.1111/exsy.12987.

[42] 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.

[43] 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.

[44] 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.

[45] S.-K. Kim, C. Y. Yeun, E. Damiani, and N.-W. Lo, “A Machine Learning Framework for Biometric Authentication using Electrocardiogram,” *IEEE Access*, vol. 7, pp. 94858–94868, Jul. 2019, doi:

10.1109/ACCESS.2019.2927079.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] T. M. Ghazal *et al.*, "Edge AI-Based Automated Detection and Classification of Road Anomalies in VANET Using Deep Learning," *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–19, Sep. 2021, doi: 10.1155/2021/6262194.

[52] 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.

[53] 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.

[54] 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.

[55] 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.

[56] 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.

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

Online: https://doi.org/10.54489/ijcim.v2i2.109 Publisher: **GAF-TIM**, https://gaftim.com

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 Is promoting the use of connected medical technologies.

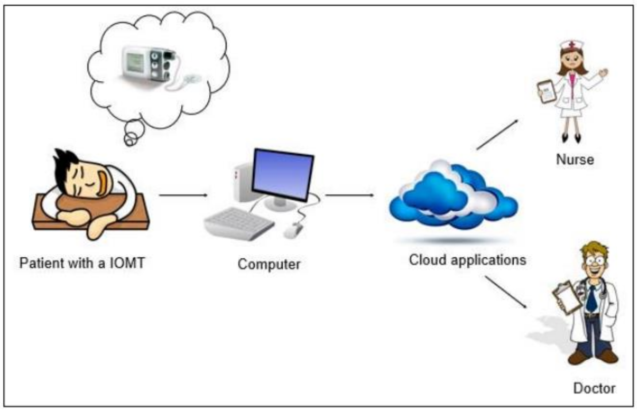


Figure 1: Internet of medical things architecture

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.

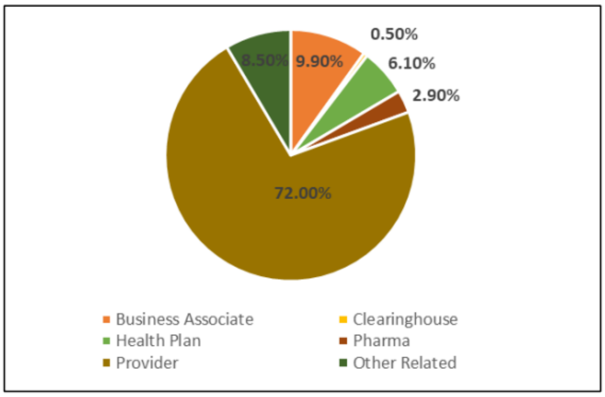


Figure 2: Organizations in healthcare compromised..

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.

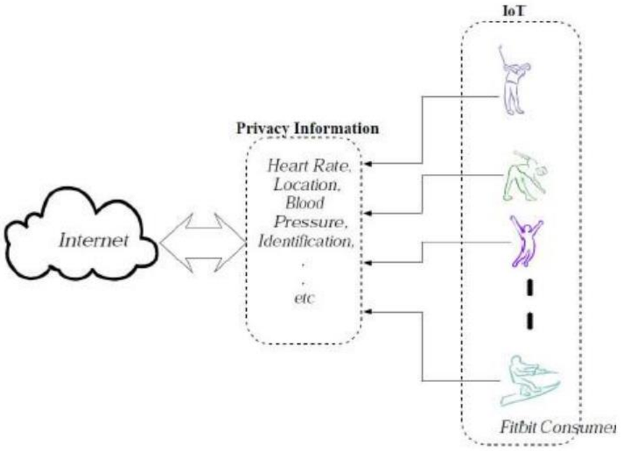


Figure 3: IOT and the security and privacy issue

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.

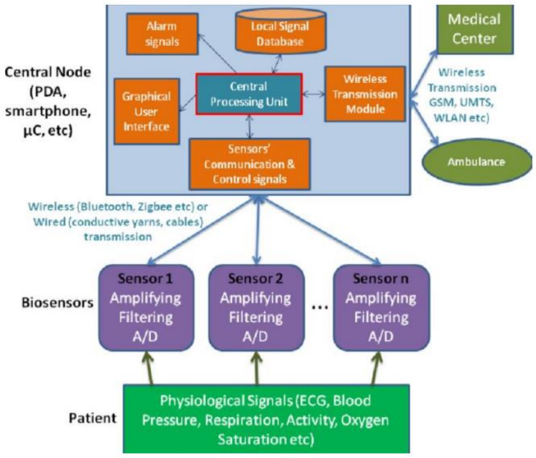

Central Node
(PDA,
smartphone,
μC, etc)
Alarm signals
Local Signal Database
Graphical User Interface
Central Processing Unit
Wireless Transmission Module
Sensors' Communication & Control signals
Medical Center
Wireless Transmission GSM, UMTS, WLAN etc)
Ambulance
Wireless (Bluetooth, Zigbee etc) or Wired (conductive yarns, cables) transmission
Biosensors
Sensor 1 Amplifying Filtering A/D
Sensor 2 Amplifying Filtering A/D
...
Sensor n Amplifying Filtering A/D
Patient
Physiological Signals (ECG, Blood Pressure, Respiration, Activity, Oxygen Saturation etc)

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.

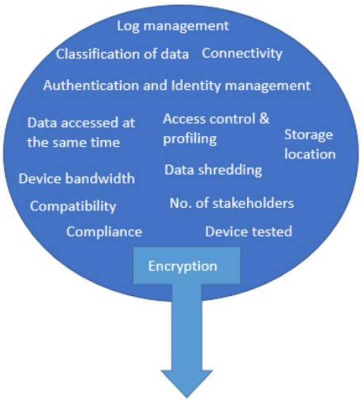
4. DATA ANALYSIS

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

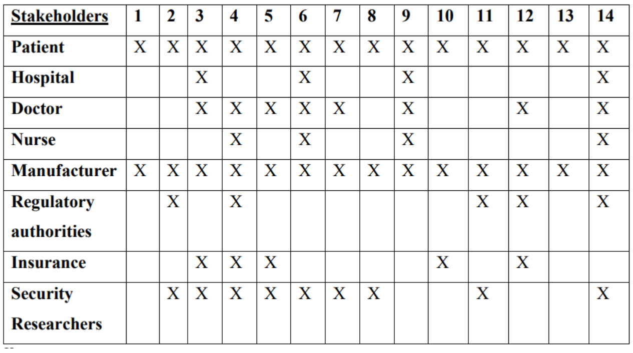
The following algorithm has been used to standardize attribute scores.

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

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.

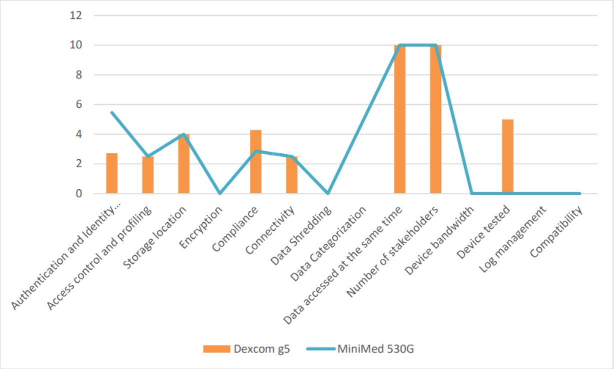


Figure 6: Comparison of two wearable IOMT devices.

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.

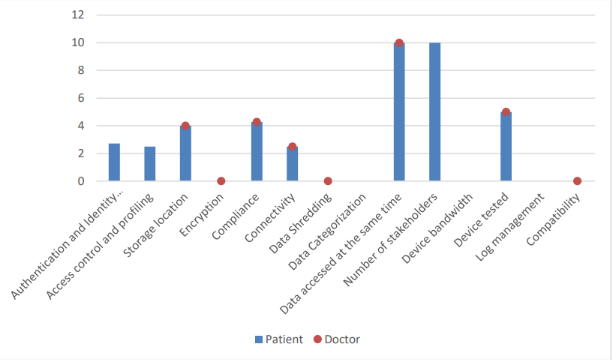


Figure 7: Comparison of a doctor and a patient for Dexcom g5.

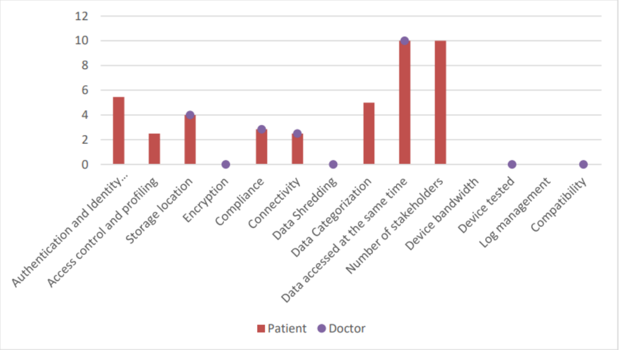


Figure 8: Comparison of a doctor and a patient for MiniMed 530G

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.

A SYSTEMATIC REVIEW ON SECURITY VULNERABILITIES TO PREVENY TYPES OF ATTACKS IN IOMT

Ahmed Bouriche

University Center of Maghnia, Algeria

ahmed89_13@yahoo.fr

ABSTRACT

And here's a summary of latest developments in Internet of Things (IoT) integrated devices, wireless connections, and biosensing which have contributed in the fast development of wearable sensor implantation. This study also discusses the applications of the internet of medical things (IoMT), which now has attracted considerable interest as an environment of networked clinical systems, computational capabilities, and medical sensors designed to improve the quality of healthcare services. The perspective of healthcare and lifestyle can indeed be totally transformed by AI technology based on 5G. The aim of this proposed research design is to investigate risks which might undermine the credibility, confidentiality, and security of IoMT platforms in consideration of the relevance of IoT platforms and 5G networks.

Moreover, there have been cutting-edge blockchain-based techniques which can aid in enhancing IoMT network security. IoMT has indeed been discovered to be vulnerable to a range of attacks, notably malware, DoS attacks, and wiretapping attacks. IoMT is additionally prone to a range of issues, involving safety, privacy, and anonymity. There are revolutionary cryptography solutions, such as password protection, authentication protocols, and data encryption, which can aid in improving the security and trustworthiness of IoMT devices despite the different of security risks.

Keywords: E-Supply, Ethics, IoMT, Blockchain.

Online: https://doi.org/10.54489/ijcim.v2i2.107 Publisher: **GAF-TIM**, https://gaftim.com

1. INTRODUCTION

Microelectron dynamic sensors and devices are one of the latest innovations in semiconductors and related technology, and the internet of things (IoT) has garnered a huge interest. Artificial intelligence (AI) is a technology used among smart devices to produce intelligent predictions [1]. These devices successfully utilize federated learning, a form of student engagement that really is suitable for Internet of Things (IoT) devices. In charge of conducting many sophisticated computation tasks, these devices should be equipped with wireless network connection [2], [3]. For with this purpose, only 5G or higher-level communications technology will provide support needed for intelligent surgical supplies [4].

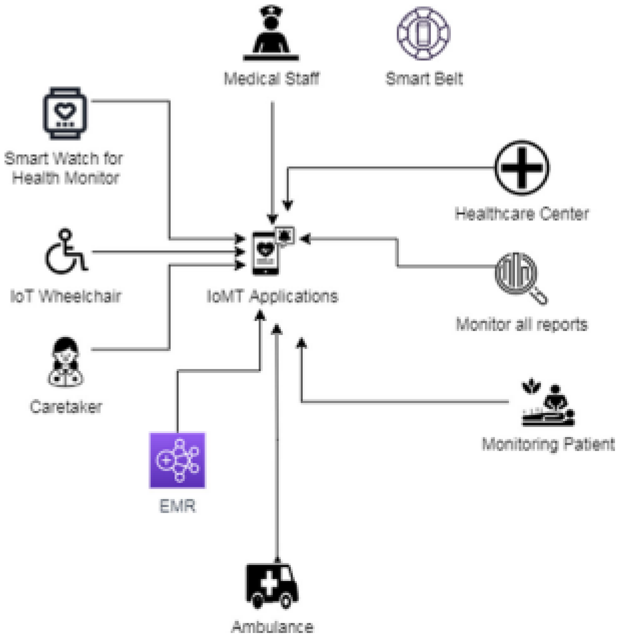


Figure 1: IoMT healthcare service applications [5].

These technologies have such a wide variety of applications irrespective of only cellphones, extending from wearable tech to healthcare monitoring [6], [7]. Even though the cost, adaptability, and throughput of the IoMT network can be considerably increased with the implementation of 5G network design [8], [9]. Despite the demanding specifications, 5G networks will be using terahertz transmissions for communication, have such a download speed of more than 1TBPS, and then use a 3-dimensional communication network (frequency, space, and time) [10] instead of a 2-dimensional structure like those found in 5G networks [11]. This one will give medical IoT devices a strong architecture with bigger and deeper coverage [12]–[14]. Blockchain support The Internet of Things (IoT) is an increasing technological concept which has interconnected billions of sentient items [15], contributing to the emergence of intelligent ecosystems comprising intelligent businesses, households, communities, and grids [16]. Among the most crucial categories for adoption of technology in the healthcare industry is the delivery of omnipresent and real-time solutions [17]. A diverse variety of entities, comprising machines, humans, and things, are interconnected into entire dataset anywhere at any any time under the IoT umbrella [18].

1.1 Problem Statement

Security breach to a patient's records may result in incorrect medications being issued, that could threaten the patient's health or possibly end in death [19], [20]. As just a consequence, however if IoMT provides great benefits, it is also vulnerable to cyberattacks like keystroke logger, extortion, and the proliferation of dangerous robots [21]. This makes the biomedical domain a crucial area for research [22], [23]. In addition to potential cyber risk, the IoMT's digitalization is vulnerable to hacking techniques that really can endanger physical security [24]. As just a consequence, a security mechanism which can safeguard the security of the IoMT network is needed for the proper integration of IoMT technology into medical systems [25]. Security is a crucial element which depends on the trustworthiness of the medical equipment [26], [27]. Identification of possible and existing vulnerabilities to the IoMT infrastructure is the very first step towards achieving this [28]. Although IoMT devices and IoT devices contain many fundamental features and characteristics [29], contemporary attacks that targeting IoT networks could also be seen as risks which might harm IoMT devices [30], [31].

2. LITERATURE REVIEW

An increasing lot of organizations have recognized that information security issues could have a negative influence on business continuity, public perception, and, in the event of noncompliance, legal authorities [32]–[34]. These dangers can also lead to loss of money and also have a harmful influence on collaborations, services to other businesses, and the satisfaction of those relationships [35]. "Data security is the safeguarding of data and the key factors contained therein, [36]" Confidential, integrity, and accessibility are the three major traits that constitute information security. Transparency is important since it controls who really can access information [37]. Information's authenticity is evaluated by just how full and unaffected it is [4], [38]. Information is considered available to customers or other organizations by the accessibility property [39], [40]. The internal factor has become a popular subject in information security for quite a while now [41]. Disappointingly, there seems to be little knowledge relevant to the topic [42]. Only outside threats, not insider exploitation, are predicted to generate revenue damage in 2008, so according 50% of those interviewed [43]–[45]. Conversely, insider exploitation also recognized by 44% of those questioned to be have happened in 2008 [46], currently the second most common type of network security fraud (after bugs) [47], [48]. Including the most current Ernst & Young survey (2009), 25percent of respondents said that there had been an upsurge in internal threats, and 13% claimed there's been a rise in internally conducted fraud [49], [50].

A worker, ex-employee, collaborator, or consumer with authorized to view an organization's resources may be using that knowledge to compromise the network security of the company or organization [51]; this is characterized as an "internal threat [52]–[54]." For so many organizations, domestic danger is a concern since employee conduct or misunderstanding can culminate in occurrences of term condition that causes, between a few lost productivity to negative press or economic damages, and also as a consequence, the organisation may not endure [55].

3. RESEARCH METHODOLOGY

The research may utilize a hybrid, subjective, or analytical methodology. While using a descriptive method, the study focused on an in-depth examination of the hypotheses which is often obtained to state or describe an occurrence utilizing open-ended methods. When a quantitative strategy is adopted, meanwhile, the research is focused on numerical or statistical information recorded to either confirm or analyze connections with any hypothesis.

3.1 IoMT Network Vulnerabities

- *Security:* IoMT systems are susceptible to network/wireless assaults since of their dependence on unsecured wireless network. Building structural flaws or insufficient security process is controlled, IoMT equipment lacked protection mechanisms, making it much easier for an opponent to intercept and overhear on the both data transfer. Additionally, so because preponderance of IoMT devices are still unable to detect and block assaults, experienced attackers can get beyond security to acquire patient records without permission. As both a consequence, attackers can just use reach a certain level to infect devices with malware or dangerous software.

- *Privacy:* The intelligence collected by IoMT devices could provide sensitive details about a participant's lifestyle. For example, as the author highlighted out, signals sent out by sensors which are intended to monitor a condition of the patient can disclose the device's medicinal expertise. Comparable to malicious activities, passive attacks like traffic monitoring allows hackers to disseminate or collect sensitive and confidential data but also patient identification. In contrast, attacks like man-in-the-middle (MitM) can undermine the safety and confidentiality of IoMT networks by interrupting with communication to transform the way two parties exchange data secretly.
- *Confidentiality:* The data obtained by IoMT devices can also provide sensitive details about a patient's lifestyle. For instance, as the researcher highlighted out, information sent by sensors which are intended to monitor a medical health can disclose the device's medical expertise. Similarly to malicious activities, attack vectors like traffic monitoring allows hackers to disseminate or collect sensitive and confidential data and also patient identification. Additionally, as highlighted by researchers, cyberattacks like man-in-the-middle (MitM) can compromise the integrity and confidentiality of IoMT networks by tampering with communication to modify the material being transferred among two parties surreptitiously.

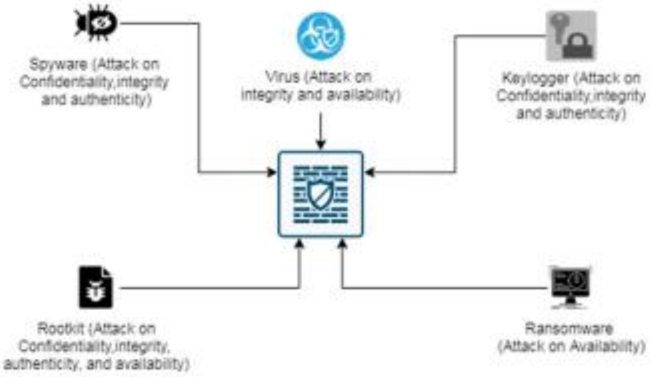

Spyware (Attack on Confidentiality,integrity and authenticity)
Virus (Attack on integrity and availability)
Keylogger (Attack on Confidentiality,integrity and authenticity)
Rootkit (Attack on Confidentiality,integrity, authenticity, and availability)
Ransomware (Attack on Availability)

Figure 2: Security Vulnerabilities in IoMT [56].

3.2 Types of Attacks in IoMT

- *Dos Attack*: The sudden uptick in fraudulent activity and attacks has made the system an unsafe place. Because modern political, social, and medicinal infrastructure is so largely dependent on networks and information technology, such attacks may have an impact on the biomedical field (IT). Security researchers have identified a large number of cyber threats and over years which might endanger cybersecurity depending on a present study. Among the most dangerous cybersecurity risks that just might jeopardize IoMT security are interruption of service (DoS) attacks. A potential hacker will make a huge number of questions in an attempt to bottleneck the computation power of a computer or wearable devices.
- *Attack of Malware:* IoMT systems also are susceptible to various types of malware, including such Trojans, infections, worms, spyware, malware attacks, and rootkits. Studies that examine the topic suggest that cyberattacks spread rapidly throughout the system by trying to take advantage of recognized or unexpected vulnerabilities. These attacks may knock down any computer system through DDoS attacks, posing a serious threat both to the integrity and confidentiality of IoMT devices. This could force a vulnerability up to a specific medical system or device to emerge. In furthermore, effective utilization of the security flaw could contribute to patient data getting destroyed, disclosed, or given unauthorized availability of medical records or IoMT devices.

- *Attack of Eavesdropping:* Among the most common known attacks for collecting data from biomedical sensors is eavesdropping. Passive eavesdropping is the terminology for when malicious attackers listen to information being transmitted in order to collect information. Furthermore, attackers may proactively overhear by making multiple friendly inquiries, which would be alluded to as proactive eavesdropping. Attackers chase down special hardware because they can intercept it and collect personal data. A patient's physiological signals could've been captured during transmission. Operations like some of those based on fingerprinting can indeed be performed out by using this data in a variety of methods. In particular, active passive attacks allow for the unlawful interruption of communication between the two organizations, including such sensor nodes or smartphones, by trying to take advantage of flaws in unsecure network.

4. CONCLUSIONS

Due to attempts to slow technological advancements, the growth of connected medical devices has changed the fundamentals of healthcare operations. Data security for medical equipment has drawn a lot of interest as a result of both factors. The adoption of cutting-edge communication technology, such as 5G networks, will completely transform the health care sector. A new paradigm in the healthcare industry will have emerged as a result of the quick development of communications technology. Tele-surgery will not be possible due to communication issues, modern healthcare framework cuts, and other factors. 5G will undoubtedly replace ambulance workers, and new technology will be reinvented. Additionally, due to advances in technology, this platform is vulnerable to a number of security problems that might seriously jeopardize patient security and privacy. Current safety concerns have motivated researchers to look into numerous medical device vulnerabilities as a result of both of these factors. Additionally, it is essential to use adequate control techniques that can maintain the security and integrity of IoMT systems because security is essential for maintaining the dependability of IoMT devices and for the successful integration of this technology into medical systems.

REFERENCES

[1] G. Raja, Y. Manaswini, G. D. Vivekanandan, H. Sampath, K. Dev, and A. K. Bashir, “AI-Powered

blockchain - A decentralized secure multiparty computation protocol for IoV," *IEEE INFOCOM 2020 - IEEE Conf. Comput. Commun. Work. INFOCOM WKSHPS 2020*, pp. 865–870, 2020, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162866.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] S. Xu *et al.*, "RJCC: Reinforcement-Learning-Based Joint Communicational-and-Computational Resource Allocation Mechanism for Smart City IoT," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8059–8076, 2020, doi: 10.1109/JIOT.2020.3002427.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] A. Yeboah-Ofori *et al.*, “Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security,” *IEEE Access,* vol. 9, no. Ml, pp. 94318–94337, 2021, doi: 10.1109/ACCESS.2021.3087109.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] S. Al-Tahat and O. A. Moneim, “The impact of artificial intelligence on the correct application of cyber governance in Jordanian commercial banks,” *Int. J. Sci. Technol. Res.*, vol. 9, no. 3, pp. 7138–7144, 2020.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[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] 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.

[44] 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.

[45] 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.

[46] 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.

[47] 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.

[48] 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.

[49] J. Almalki *et al.*, "Enabling Blockchain with IoMT Devices for Healthcare," *Information*, vol. 13, no. 10, p. 448, 2022, doi: 10.3390/info13100448.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] C. Lee and G. Ahmed, "Improving IoT Privacy, Data Protection and Security Concerns," *Int. J. Technol. Innov. Manag.*, vol. 1, no. 1, pp. 18–33, 2021, doi: 10.54489/ijtim.v1i1.12.

[56] S. Pandey, R. K. Singh, A. Gunasekaran, and A. Kaushik, “Cyber security risks in globalized supply chains: conceptual framework,” *J. Glob. Oper. Strateg. Sourc.*, vol. 13, no. 1, pp. 103–128, 2020, doi: 10.1108/JGOSS-05-2019-0042.

INVESTIGATING THE IMPORTANCE OF ETHICS AND SECURITY ON INTERNET OF MEDICAL THINGS (IoMT)

Asaad Ali Karam

Associate Professor, University of Duhok, Iraq

asaad.ali@uod.ac

ABSTRACT

Numerous opportunities are emerging due to the Internet of Things' (IoT) rapid development, which has the potential to significantly improve human quality of life in many areas. The healthcare industry is the main place where IoT can enhance our quality of lives. Security and privacy concerns, however, take center stage in electronic health (eHealth) systems, and the incorporation of IoT makes them increasingly difficult to address. Due to the numerous stakeholders in its broader ecosystem, the majority of IoMT which raises security concerns. The IoT-based healthcare system has various security features. This search provides an Identity-Based Cryptography cornerstone management technique that uses collaborative authentication and a secret passcode to protect transformation of data between any IoT health device and any other entity from a different company or domain (IBC).

***Keywords*:** Ethics, Security, Internet of Medical Things (IoMT).

1. INTRODUCTION

The delivery of health care services has changed as a result of the IT and medical industries' convergence, or eHealth. E-Health provides a fresh method of using health resources, such as data, cash, and pharmaceuticals. It assists all concerned parties in making better use of those resources [1]. According to the McKinsey Global Institute, IoT-based hospitals applications will have the greatest economic impact compared to other IoT apps by 2025, growing the global economy by between 1.1 and 2.5 trillion dollars annually [2]. It demonstrates that IoT hospitals has a highly promising result. In terms of the advantages it will

Online: https:// doi.org/10.54489/ijcim.v2i2.114

bring to individuals, technology, and the economy [3]. Despite all the positive information regarding IoT-based healthcare solutions, security and privacy remain major issues [4], [5].

IoT-based hospital systems face numerous security plus privacy challenges, including hackers attack, security of the communication channel and ecosystem (such as multi-factor authentication, key management, and cryptographic support), and stealing attempts of the stored information, etc [6]. Yet, the Health Insurance Portability and Accountability must be complied with any IoT device that transmits patient health information (HIPAA). The limited power, processing, and memory capabilities of IoT devices also indicate that the security mechanism must make effective use of those resources [7]. Additionally, the design of IoT-based health care systems generally comprises a number of stakeholders that are members of several organizations with varying security domains and policies, which makes the security work more challenging [8].

In light of the above-described conditions, it is crucial to offer serious management that facilitates multiple methods and safe data transfer among devices within the IoT-based health care system [9].

This research provides an IBC-based security system that help all previously mentioned functionalities. The Identity Based encryption topic was selected considering it is essentially an asymmetric key scheme, which is simpler to distribute keys for [10]. Additionally, unlike other asymmetric key schemes, such as Elliptic Curve Cryptography, it does not need a certificate for practical key distribution. The method, which was created using a variation of Identity Based Encryption that fixes the key escrow issue in the Identity Based cryptography, offers mutual authentication and agreement for secure connection entities across various companies or domains[11].

2. LITERATURE REVIEW

2.1 Safety Challenges and Solutions

The security issues with the IoT-based healthcare system are discussed in this section. There are two primary kinds of challenges: those relating to the inherent nature of the IoT, which has an influence on security solutions; and those relating to IoT system security, particularly in the domain of health care [12]. Additionally, a few potential answers to the problems discussed are offered based on some related publications. Low-speed CPUs are built into Internet of Things health devices [13]. Such gadgets have a slow central processing unit

(CPU) that isn't particularly powerful. Additionally, computationally intensive operations cannot be carried out by these devices [14]. They only serve as a sensor or actuator, in other words. Therefore, it might be difficult to identify a security solution that enhances security performance while minimizing resource usage [15]. However, as the number of IoT devices has increased steadily, more and more devices are joining the world data network. Therefore, creating a highly scalable security system without sacrificing security standards is a different difficult task. Medical records include extremely confidential information regarding a patient's data and health statues that needs to be kept safe and secret from any hackers [16], [17].

In order to comply with HIPAA, hospitals and other healthcare organizations must securely communicate patients' sensitive information [18]. If the automated data gathering isn't validated and handled appropriately, security breaches and privacy violations are quite likely due to the widespread and omnipresent nature of IoT [19]. Without real-time monitoring, patients' private and sensitive medical information may be altered, misused, or compromised. This poses a grave threat to infrastructure in addition to having a devastating effect on people's lives. Apps and wearable technology might be taken over by malicious users, who could then access users' sensitive information and pose grave security and health threats [20]. In order to comply with HIPAA, hospitals and other healthcare organizations must securely communicate patients' sensitive information. If the automated data gathering isn't validated and handled appropriately, security breaches and privacy violations are quite likely due to the widespread and omnipresent nature of IoT [21].

Without real-time monitoring, patients' private and sensitive medical information may be altered, misused 43, or compromised [22]. This poses a grave threat to infrastructure in addition to having a devastating effect on people's lives. Apps and wearable technology might be taken over by malicious users, who could then access users' sensitive information and pose grave security and health threats [23].

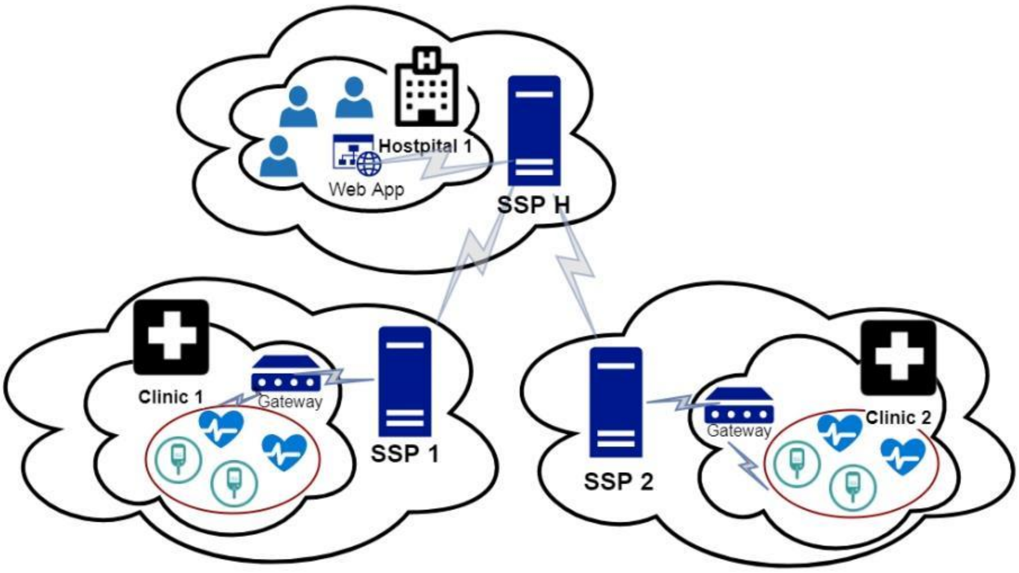


Figure 1. Reference architecture of IoT-based health care across domains

The management of passwords and access to applications and private patient data presents another difficulty [24]. When a patient's sensor gadget asks for access, for example, medical care providers are permitted to do so, but the internet connection sources may be an insecure Wi-Fi network that is readily compromised [25].

Numerous authentication approaches might be used to enable patients to confirm their identities and grant doctors' access to their internally implanted gadgets [26], but suddenly they lost consciousness and are still in severe need of medical treatment and direction [27]. Some manufacturers of IoT healthcare products offer a lifetime difficult password to managing IoT devices [28], the device documentation contains passwords that are accessible to the general public and might be used to incorrectly set the device, endangering the lives of patients [29]. Correctly establishing and executing cryptography methods in IoT health is another difficulty. Due to the ubiquitous and ongoing capabilities of the IoT, Cryptographic key management is necessary yet complex [30].

The IoT platform necessitates the use of concurrent authentication processes with real-time answers. Health information about patients should be encrypted and decrypted whenever it is judged necessary, according to HIPAA regulations regarding Transmission Security Encryption (TSE) [31]. Entities are required to create documentation of the installed encryption technology, including rules and protocols, the exchange of cryptographic key management, and limiting who has access to generate and modify cryptographic keys. Additionally, it's important to audit and enforce policies for keeping and sharing keys that really are secret [32]–[34].

A lot of security measures have been developed to solve IoT-related issues in various apps; these plans may also be used in the healthcare industry [35]. Given that IoT comprises of constrained-devices (e.g., limited processing) [36]. The issue of secure transmission in IoT as specified by HIPAA law is inextricably linked with cryptographic methods, as are huge numbers of IoT nodes, which has expanding issues [37]. Furthermore, proper encryption management is critical in secure communication and is tied to authentication.

Due to its tiny key size and ability to meet the needs of constrained devices, symmetric key cryptography-based schemes were first the subject of in-depth research [38]. However, it has a significant scalability flaw [39]. There have also been various attempts to implement a Public Key Cryptography (PKC)-based system on restricted devices in order to overcome the scalability issue [40]. It has been demonstrated that it is possible to implement PKC with restricted hardware, particularly when utilizing ECC, which necessitates a smaller key size than RSA-based PKC [41].

However, standard PKC requires credentials, which take up more memory and are difficult to handle. A certificate less PKC system called IBC has been developed to address this issue [42]. The fundamental concept of the original IBE is as follows: initially, a central entity known as the Private Key Generator (PKG) is in charge of producing some public consideration and a core key that is kept a secret [43]. Following that, all other people that trust the specific PKG given their Identifications users can produce their own private keys using the master key [44]. With the exception that the public key can be created by any entity using a known ID, the encryption-decryption procedure can now be carried out in the same way as the conventional PKG. Due to its advantages, e.g. Some IBC-based security approaches, such as certificate less and minimal resource needs, have also been deployed for restricted devices, including Mobile Ad-hoc Networks [45]. Random strings, such as the identity of a communicating party, can be used as a public key in IBC, taking the certificate in conventional PKC place [46].

IBC plan has been put out for the Internet of Things. It is suggested to use a proxy and a key setup mechanism for two interacting entities, one of which is a restricted device [47]. Machine-to-Machine (M2M) IBC protocol design pattern was put out in reference [48].

2.2 Safety challenges and solutions. Part2

This section explores potential IoT-based hospital system design from multiple aspects [49]. Has investigated the interaction of four parties—sensor owners, sensor publishers, extended service providers, and sensor data consumers is the foundation for how IoT sensing devices work in general [50]. SO might be a business that sells sensors, a government agency, a private individual, or another SO [51].

If the SO concludes that data produced by these sensors will really be accessed on the cloud, it must define the data access policy that all SPs should implement and potential users should follow [52]. When an SDC (for example, a government agency, a business enterprise, an academic institution, or an employee) expresses interest in data exchange from a published sensor, the SP mediates the establishment of a service agreement between the SDC and the relevant SO, outlining the SO's obligations with regard to the importance and accessibility of the submitted sensing data, as well as their adherence to current standards [53].

Sensing Service Provider (SSP) is a different organization that streamlines communication between SDC and also other organizations that serve its goals, such as SO (for data accessibility, integrity, and quality), SP (for access services to sensor data), and other extended service providers (for value added services) [54]. In a scenario involving health care, SDC might be any supplier of health care services or a medical facility (such as a hospital, clinic, etc.). Those SDC in the healthcare industry may choose to adopt IoT-based hospital services for addition to their current IT infrastructure or by outsourcing it to specialist providers depending on the financial, human, and technological resources that are available [55]. Particularly for tiny medical institutes, the second choice might be more preferred (e.g. clinics, general practitioners).

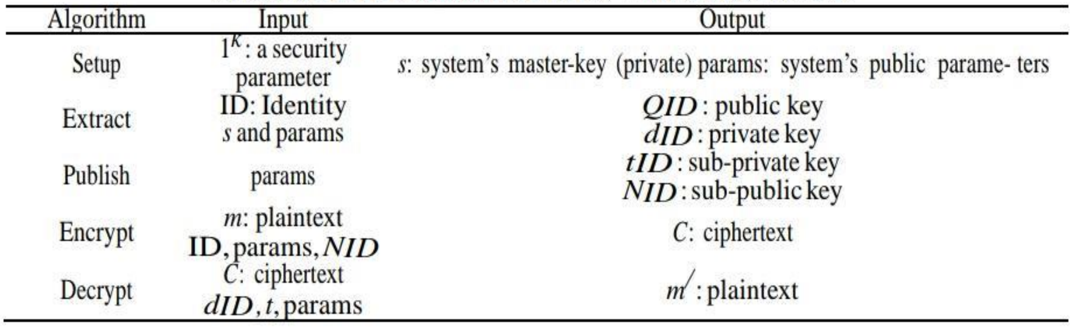
From a practical standpoint, the architecture deployment strategy of an IoT-based hospital system may be done in a variety of ways . According to one of the studies, tele-EKG!, an ongoing tele-health pilot project, is done in such a way that a renowned cardiac hospital serves as the initiative's hub while also providing services to other distantly placed healthcare providers [56]. To get a diagnosis relating to the cardiac difficulties of the patients in the distant region to health care providers who lack cardiology doctors may submit the EKG test data of their patients to other cardiologist who is a member of the referring hospital using tele-EKG.

The example model is a condensed form in which SP is taken to be the SSP itself, the SO is a component of the healthcare providers (clinics one and two), and hospital 1 is the SDC.

Additionally, it is presumable that every healthcare organization hired expert providers to handle the IoT-based healthcare system (e.g., SSP 1, SSP 2 and SSP H).

According to table 1, the reference architecture will feature three PKG for each SSP domain in accordance with the planned IBC security system, which calls for PKG. PKG is only accessible to organizations that are part of its domain for security reasons. They provide public parameters and master secret keys for each domain as PKGs.

TABLE 1.
SUMMARY OF ALL ALGORITHMS IN IBE WITHOUT KEY ESCROW



Algorithm	Input	Output
Setup	1^K: a security parameter	s: system's master-key (private) params: system's public parame- ters
Extract	ID: Identity s and params	QID : public key dID : private key
Publish	params	tID : sub-private key NID : sub-public key
Encrypt	m: plaintext ID, params, NID	C: ciphertext
Decrypt	C: ciphertext $dID, t,$ params	m' : plaintext

3. MTHODOLOGY

The definite purpose of the research projected by exploring secondary data from previously published journals, books and literature whereas, this research was primarily hold to signify Identity-Based Cryptography that is a cornerstone management strategy secures data translation between any IoT health device and any other entity from a different business or domain by using cooperative authentication and security.

4. EMPIRICAL ANALYSIS

4.1 IBE Scheme

Several researchers argued, the suggested system is based on an IBE variation without key escrow. Franklin's original IBE method uses four randomized algorithms—Setup, Extract, Encrypt, and Decrypt—while the IBE's variation without key escrow includes a fifth algorithm called Publish. The last table contains a summary of the inputs and outputs for all five methods.

And by taking note that the setup algorithm runs completely in the PKG, which may happen, for example, during system startup. As part of the Extract algorithm, the PKG gets an

AI input ID from a communicating entity. Once the algorithm is carried out in the PKG, QID is made public in a directory while dID is provided covertly to the communicating entity. The remainder of the algorithm (Publish, Encrypt, and Decrypt), with the exception of NID being one of the outcomes of the Publish process being published in a public directory, occurs in the communicating entity.

Before describing the other process in the suggested approach, namely key agreement authentication and system and device initialization. Table 2 provides definitions for the notations used in the suggested scheme.

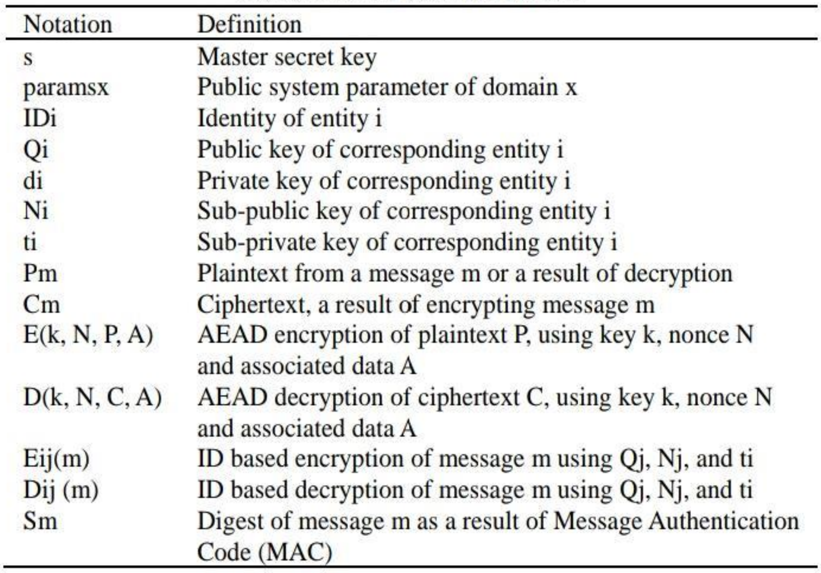
4.2 System and Device Initialization

Framework administration is the operation performed when a gateway and a constrained device join the SSP!, although system initialization is a method performed when an SSPPKG !'s is enabled. The most important step in configuration is generating the master key and parameters, followed by making the parameters public, as mentioned in the prior section. Furthermore, the SSP PKG is dependent on it! to have a unique online identity that can be recognized by anything or anybody As a result, we recommend that the IoT Service Provider's primary identity be the domain name, to which the device identity will be attached. Even if the access points is in a different domain, having such an identifier scheme is helpful in the lookup process.

Mainly two operations must be carried out: the production and distribution of the gadget by the PKG, and the formation of sub-public and sub-private key pairs by the device itself. In theory, the device's identification and accompanying private key are distributed statically during the flashing period of the device, but the online technique may be done more dynamically. In this situation, an online approach is selected, and a secure method of providing the device's private key is suggested.

Two identical keys, KlnitReq plus KlnitRsp, which are generated one time randomly and will be useless after device initialization, are used to secure the proposed online device initialization. There are several ways to get the keys. One useful method is to register a device via a web interface. After the registration procedure, the registered device will receive a unique device identification, KlnitReq, and KlnitRsp (e.g. they can be loaded to the device by cable data after downloading from PKG). It is now able to add more human-friendly names to the unique device identification, such as the type of device (gateway, EKG, diabetes sensor, etc.). The position of the device (hospital or clinic, etc.). Then, utilizing Authenticated Encryption with Associated Data, the device may safely ask for its identification and associated private key (AEAD). AEAD was chosen because it works quicker than a safe implementation of Hash-based Message Authentication Code (HMAC), which uses two keys for encryption and authentication, and it is more secure to fully authenticate the cipher text rather than just encrypt it. Table 2 displays the whole secure device initialization process.

TABLE 2.
DEFINITION OF USED NOTATIONS



Notation	Definition
s	Master secret key
paramsx	Public system parameter of domain x
IDi	Identity of entity i
Qi	Public key of corresponding entity i
di	Private key of corresponding entity i
Ni	Sub-public key of corresponding entity i
ti	Sub-private key of corresponding entity i
Pm	Plaintext from a message m or a result of decryption
Cm	Ciphertext, a result of encrypting message m
E(k, N, P, A)	AEAD encryption of plaintext P, using key k, nonce N and associated data A
D(k, N, C, A)	AEAD decryption of ciphertext C, using key k, nonce N and associated data A
Eij(m)	ID based encryption of message m using Qj, Nj, and ti
Dij (m)	ID based decryption of message m using Qj, Nj, and ti
Sm	Digest of message m as a result of Message Authentication Code (MAC)

4.3 Authentication Mechanism with Key Agreement:

Form three depicts a situation when the suggested authentication procedure and key agreement are used. In this example, user A of a mobile app wishes to access sensor B, which is a part of an IoTSP domain. User A and sensor B shall be referred to as A and B, respectively, moving forward for the sake of simplicity. Additionally, the access point to B for A is the IoT Server (IoTS). Since it is anticipated that the mobile app (either the app itself or the server that offers API to the app) performs action A in this situation, it is represented in form 3 as a single entity. Additionally, it may be believed that practically speaking, entities within each domain are unaware of the system parameters and sub-public keys of entities inside other domains, necessitating a lookup operation prior to encryption. Following is an explanation of the authentication technique in detail:

First, using IDIoT S = H1IoT SP (IDIoT S), where H1IoT SP is a part of paramsIoT SP, A does a search to acquire NIoT S and paramsIoT SP. For encryption, additional paramsIoT SP parameters are also utilized. Then, using QIoT s, NIoT s, and tA as keys, IDA, IDB, and timestamp T are encrypted to generate C1. Here, T is utilized to stop a counterattack. IDA, IDIoT S, and C1 are then sent to IoTS.

IoTS will conduct a quest depending on the IDA obtained after receiving a message from A in order to acquire the parameters A and NA. After a successful search, it decrypts C1 to produce IDA, IDB, and T using dIoT S, tIoT S, and N A. Then T is validated, and IDA is checked to see whether it is comparable to the one that was received. If they are true, the procedure continues; if not, it pauses and notifies A of the problem. A message containing NB is encrypted as C2 using QA, NA, and tIoT S after successful validation, and C2 is then delivered to A. A second message containing the parameters A and NA is encrypted as C3 using QB, NB, and tIoT S before being delivered to B, letting A know that they want access to it.

After receiving C2, A uses dA, tA, and NioT S to decode it in order to produce NB. A then creates nonce A, encrypts it with IDA using QB, NB, and tA as C4 before sending it to B.

B decrypts C3 after receiving it from IoTS in order to get the parameters M A and NA utilizing dB, tB, and NioT S.

B decrypts C4 using dB, tB, and NA after receiving it from A in order to produce nonceA. Then, using a key derivation function, such as an HMAC-based Key Derivation Function, B creates nonceB and uses it, together with nonceA and IDB, to create the shared secret key with A, kBA (HKDF). After that, IDB and nonceB are encrypted using QA, NA, and tB as C5, and a digital S1 is made from a message made up of IDB, IDA, and nonceA with key KBA using a message authentication code like HMAC. IDB, IDA, C5, and S1 are then sent to A.

A receives C5 and S1, decrypts C5 using dA, tA, and NB to derive nonceB, and then generates KBA using nonceA, nonceB, and ID. Next, using the newly constructed kBA, another S/ is formed in the same manner that B did it, and it is then validated against the received S1. Following S1's verification, S2 is produced using IDA, IDB, and nonceA using kBA and delivered to B.

S2 is then validated by b when it has been received. Both A and B will use kBA as their shared secret key after successful verification.

User A and sensor B are ultimately together are authenticated. Additionally, they may communicate privately and securely using symmetric key encryption, such as Advanced Encryption Standard (AES), which has kBA and is more compact than public key encryption.

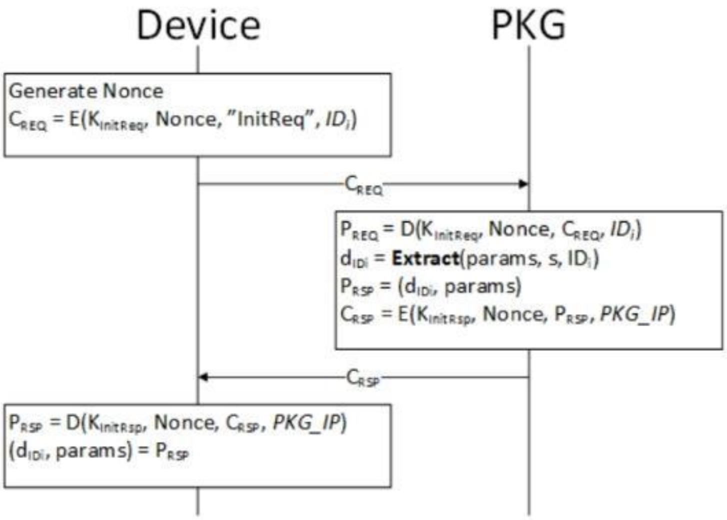

Device
PKG
Generate Nonce
C_{REQ} = E($K_{InitReq}$, Nonce, "InitReq", ID_i)
C_{REQ}
P_{REQ} = D($K_{InitReq}$, Nonce, C_{REQ}, ID_i)
d_{IDi} = **Extract**(params, s, ID_i)
P_{RSP} = (d_{IDi}, params)
C_{RSP} = E($K_{InitRsp}$, Nonce, P_{RSP}, PKG_IP)
C_{RSP}
P_{RSP} = D($K_{InitRsp}$, Nonce, C_{RSP}, PKG_IP)
(d_{IDi}, params) = P_{RSP}

Figure 2. Device initialization protocol in a SSP! Domain

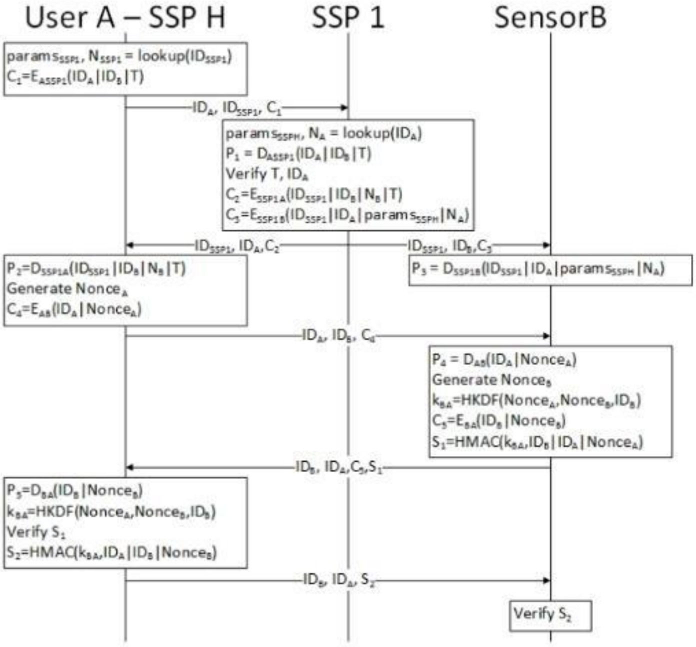

User A – SSP H
SSP 1
SensorB
$params_{SSP1}$, N_{SSP1} = lookup(ID_{SSP1})
C_1=E_{ASSP1}(ID_A|ID_B|T)
ID_A, ID_{SSP1}, C_1
$params_{SSPH}$, N_A = lookup(ID_A)
P_1 = D_{ASSP1}(ID_A|ID_B|T)
Verify T, ID_A
C_2=E_{SSP1A}(ID_{SSP1}|ID_B|N_B|T)
C_3=E_{SSP1B}(ID_{SSP1}|ID_A|$params_{SSPH}$|N_A)
ID_{SSP1}, ID_A,C_2
ID_{SSP1}, ID_B,C_3
P_2=D_{SSP1A}(ID_{SSP1}|ID_B|N_B|T)
Generate $Nonce_A$
C_4=E_{AB}(ID_A|$Nonce_A$)
P_3 = D_{SSP1B}(ID_{SSP1}|ID_A|$params_{SSPH}$|N_A)
ID_A, ID_B, C_4
P_4 = D_{AB}(ID_A|$Nonce_A$)
Generate $Nonce_B$
k_{BA}=HKDF($Nonce_A$,$Nonce_B$,ID_B)
C_5=E_{BA}(ID_B|$Nonce_B$)
S_1=HMAC(k_{BA},ID_B|ID_A|$Nonce_A$)
ID_B, ID_A,C_5,S_1
P_5=D_{BA}(ID_B|$Nonce_B$)
k_{BA}=HKDF($Nonce_A$,$Nonce_B$,ID_B)
Verify S_1
S_2=HMAC(k_{BA},ID_A|ID_B|$Nonce_B$)
ID_B, ID_A, S_2
Verify S_2

Figure 3. Authentication mechanism with entity in different domain

5. RESULTS AND DISCUSSION

The security capabilities of the suggested approach are discussed in this chapter. The threat model used for the security study is provided first. The suggested scheme's security aspects are next examined. Finally, a discussion on mutual authentication's security is had.

5.1 Risk Model

Every message sent through the system is eavesdropped on by an outside attacker who then replays the previous message to the receiver, breaks up the eavesdropped message into smaller pieces, reassembles the pieces into a new message, and sends the new message to any legal entity. The attacker can also decrypt ciphertext if they have access to the corresponding key, modify the decrypted plaintext, and forge messages using the public key of a legal entity.

Compromised equipment, such one that can perform all actions an outside attacker might, uses its own private key, which was given with MSP, to decode intercepted messages or create fake ones. A compromised SSP that uses its own private key to decode intercepted messages or create fake messages and is able to do any action an outside attacker could.

- *Security Feature of The Proposed Scheme*

When a communication is encrypted, it is authenticated: Sender I must use ti to encrypt the message before sending it to receiver j, and the recipient must use Ni to decode the message. The message could only be properly encrypted and decrypted with the right (ti,Ni) combination. This indicates that the recipient could only decode the message by the matching Ni if the communication was encrypted by an authorized sender i. Therefore, the encryption serves as the message's authentication, and no more signatures are required.

The key escrow issue is solved by using dj and tj when a receiver j wishes to decode a message. The receiver is the sole party with knowledge of the dj, SSP, and tj. The message could therefore only be decoded by the recipient because to the tj even if the SSP is hacked or the private key dj is exposed. The primary escrow issue is thus resolved by the presence of tj. Likewise, the update of data strengthens the authentication scheme's security.

- *Mutual Authentication*

The authentication technique enables mutual authentication between a hospital user, a medical sensor, and the SSP1! The SSP1! verifies the hospital user's ID. The SSP1 and its associated sub-public key NID could only decipher messages encrypted by authorized hospital users. Additionally, the sub-secret key tID makes sure that only the authorized mobile user may authenticate a message with encryption, and that only the target sensor can decode a message and vice versa.

6. CONCLUSION

IoMT security and privacy assurance is a really difficult task. The fact that IoT is mostly used to link patients with medical institutions or among a number of healthcare providers spread across several sectors with various levels of trust authority makes it more difficult. An IBC-based system has been put forth for the purpose of securing communication in IoMT across several domains. The key contributions are the IBE-based key-escrow-free authentication mechanism, the mechanism to look up IBE system parameters in other domains, the mechanism to generate shared secret keys to secure communication of the presentation of the mutual authentication.

A cryptographic identity might be used alternatively of a plain identity to facilitate verification and increase identity security, but this is still up for debate. In order to take into account more stakeholders as described in the suggested model, an extension of the proposed scheme with an expanded IoT-based health care system architecture needs to be taken into consideration. To test the effectiveness and practical viability of the suggested method, it will also be implemented in a prototype or genuine IoT system.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] R. Bose, H. Mondal, I. Sarkar, and S. Roy, “DESIGN OF SMART INVENTORY MANAGEMENT SYSTEM FOR,” *e-Prime - Adv. Electr. Eng. Electron. Energy*, p. 100051, 2022, doi: 10.1016/j.prime.2022.100051.

[13] 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.

[14] 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.

[15] 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.

[16] M. Alazab, S. Alhyari, A. Awajan, and A. B. Abdallah, “Blockchain technology in supply chain management: an empirical study of the factors affecting user adoption/acceptance,” *Cluster Comput.*, vol. 24, no. 1, pp. 83–101, 2021, doi: 10.1007/s10586-020-03200-4.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] E. Al Alkeem, D. Shehada, C. Y. Yeun, M. J. Zemerly, and J. Hu, “New secure healthcare system using cloud of things,” in *Cluster Computing, , Vol. 20, No. 3,* 2017, pp. 2211–2229.

[22] 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.

[23] 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.

[24] 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.

[25] A. Kumar, K. Abhishek, P. Nerurkar, M. R. Khosravi, M. R. Ghalib, and A. Shankar, “Big data analytics to identify illegal activities on Bitcoin Blockchain for IoMT,” *Pers. Ubiquitous Comput.*, 2021, doi: 10.1007/s00779-021-01562-z.

[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] 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.

[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] 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.

[30] 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.

[31] 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.

[32] P. Velmurugadass, S. Dhanasekaran, S. Shasi Anand, and V. Vasudevan, “Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm,” *Mater. Today Proc.*, vol. 37, no. Part 2, pp. 2653–2659, 2020, doi: 10.1016/j.matpr.2020.08.519.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] G. Al-Naymat, H. Hussain, M. Al-Kasassbeh, and N. Al-Dmour, "Accurate detection of network anomalies within SNMP-MIB data set using deep learning," *Int. J. Comput. Appl. Technol.*, vol. 66, no. 1, pp. 74–85, 2021.

[45] 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.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] M. Abu-Arqoub, G. Issa, A. E. Banna, and H. Saadeh, "Interactive Multimedia-Based Educational System for Children Using Interactive Book with Augmented Reality," *J. Comput. Sci.*, vol. 15, no. 11, pp. 1648–1658, 2020, doi: 10.3844/jcssp.2019.1648.1658.

[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.