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

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.