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.

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].

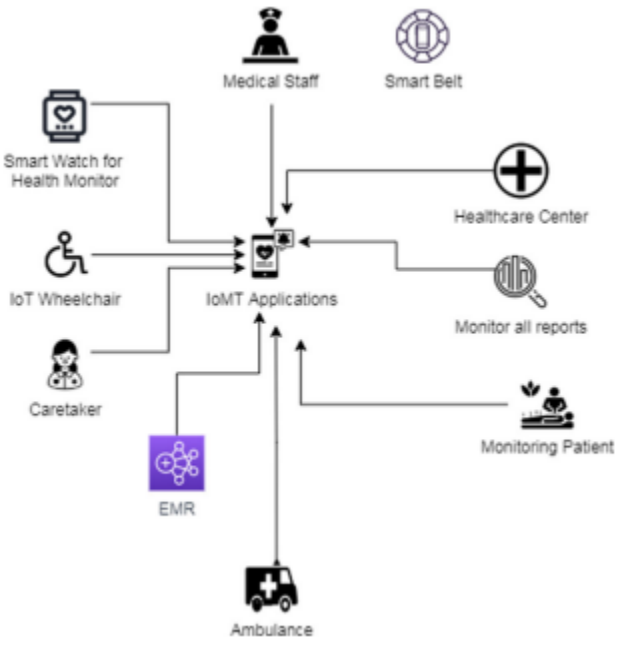

Figure 1: IoMT healthcare service applications [5].

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 non-

compliance, 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.

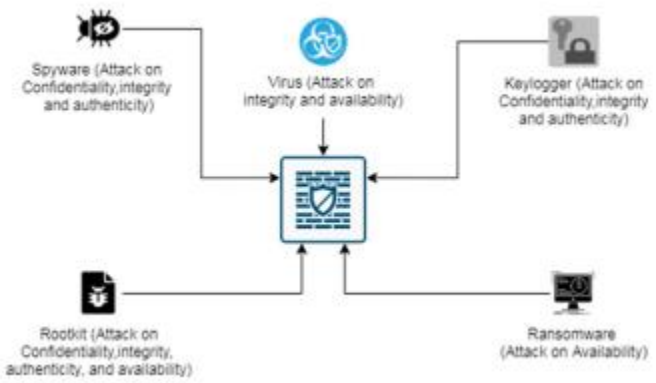

Figure 2: Security Vulnerabilities in IoMT [56].

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.