Deggendorf Institute of technology

Bachelor : Artificial Intelligence

Sustainable Approach to IoT Monitoring in Remote Working and Ethical Considerations: A Literature Review

Mahmoud Haroun

Matriculation Number: 22111275

Semester: 3

Prof. Dr. Javier Valdes

Sustainable Approach to IoT Monitoring in Remote Working and Ethical Considerations: A Literature Review

Abstract – **The prevalence of IoT monitoring in remote working is based on the need for organizations to improve productivity through process and employee monitoring. The associated sustainable approaches primarily involve waste cost and reduction possible through real-time management of business processes and employee practices. This literature reviews summarize critical findings on the adoption of IoT monitoring in organizational settings with a primary focus on how the underlying digital solutions impact a company's workforce. The study synthesizes findings from peer-reviewed journals published in the last seven years. It addresses the role COVID-19 pandemic in remote working, the prevalence of IoT monitoring, waste and cost reduction in IoT-driven management, and ethical considerations. While the pandemic spearheaded the widespread adoption of remote working, organizations stuck to the work setting based on its promising opportunities, further integrating IoT monitoring. Even though IoT-based surveillance enhances process efficiency, the underlying ethical considerations are still open to debate. IoT monitoring raises privacy and confidentiality concerns as some employees are uncomfortable sharing their private data with the company.**

Keywords: **IoT monitoring, ethical considerations, remote working**

I. Introduction

Digital technologies drive organizational functions across multiple domains, including manufacturing, healthcare, research and development, sales and marketing, and, most importantly, communication. Organizations use technology however they see fit, mainly improving production processes and lowering operational costs through system automation. Nagy et al. [1] delineated that the fourth industrial revolution (Industry 4.0) – an innovative and qualitative revolution – heavily relies on adequate data. Before the inception of data-driven decision-making through data analytics, organizations relied on experts for informed choices. Technology changed business practices through decision support systems and big data analytics, allowing fewer experts to manage critical operations based on computerized expert systems [1]. Better even device interconnections enable organizations to monitor essential aspects of employee functions and inventory management. Device interconnectivity adopts the Internet of Things (IoT) concept and associated surveillance techniques. IoT-based devices seamlessly exchange data, enhancing big data analytics through data science for actionable insight.

IoT refers to digital devices embedded with sensors and smart applications for efficient data interchange [2]. IoT in the workplace involves sensors and address monitoring capabilities for supply chain and process management within business systems [1]. IoT-enabled devices help businesses use technology to monitor products and employee services to improve service delivery. Managers can track employee practices using desktop and mobile applications and related IoT monitoring technologies to transmit real-time activity data. Also, IoT facilitates the adoption of remote working, primarily working from home or anywhere outside business premises [3], [4], to ensure employee competence and improved productivity. IoT monitoring monitors and manages connected devices, staying updated on current business processes, ultimately limiting time and resource wastage [1]. IoT monitoring is central to sustainable manufacturing, processing, and service delivery through the waste reduction in system processes. Even though IoT-based surveillance enhances process efficiency and overall productivity in the supply

chain and business processes, the underlying ethical considerations are still open to debate. Therefore, it is essential to explore the benefits of IoT monitoring in remote working, grounded on sustainability, and the ethical considerations since associated technologies involve human use and interaction with machines.

This literature review summarize critical findings on the adoption of IoT monitoring in organizational settings with a primary focus on how the underlying digital solutions impact a company's workforce. The study considers sustainability in light of system processes and employee practices. It also covers ethical issues based on industry regulations and personnel perspectives. The remainder of this paper involves the methodology (Section 2), which summarizes the data collection approach, the discussion (Section 3), which covers the literature review; and Section 4, which concludes the paper and summarizes significant findings.

II. Methodology

The study summarizes previous publications on IoT monitoring in remote working based on sustainable and ethical constraints. The methodology involves data collection, Phase I, and synthesis of sources to findings, Phase II. In Phase I, secondary sources, primarily peer-reviews journal articles, were gathered from online databases (digital libraries), including Google Scholar, Science Direct, JSTOR, and IEEE Xplore. The focus on recent publications was mainly influenced by the widespread adoption of remote working recently. The applied inclusion-exclusion criteria considered sources published in the last seven years – from 2017 to date. Sources published before 2017 were excluded. Any reference to qualify for inclusion must have been published in English. The literature search involved keywords like "IoT monitoring," "remote working," "ethical considerations," and "sustainability." Phase II involved analyzing sources and grouping them based on similarities. Sources were categorized based on titles and partly on shared themes. That way, it was practical to explore sources addressing specific issues collectively. Zotero Reference Manager was instrumental in analyzing and citing sources.

II. Discussion

A. Role of COVID-19 in Remote Working

Organizational leaders should acknowledge the role of the COVID-19 pandemic in remote working arrangements compared to the willingness and preparedness of companies since it influences IoT monitoring and remote working [4]. Following the prevalence of the COVID-19 pandemic in early 2020, several organizations embraced remote working, leveraging the underlying benefits like time-saving in high road traffic zones and convenience and flexibility for people whose jobs do not involve social interactions. Even though the widespread adoption of remote working due to COVID-19 was primarily triggered by the disease' containment measures, many organizations began benefiting from the underlying benefits regarding operations efficiency. Without the pandemic, it may have taken the companies longer to consider remote working initiatives.

Corporations need massive resources to deploy and manage remote working and IoT-based resources. Besides the fundamental skillsets, employees need mental and psychological preparation and technology acceptance to adjust to the new business technologies and remote working functions [5]. The COVID-19 pandemic has triggered most ongoing remote working arrangements since 2020. At the pandemic's peak, most organizations were not ready for remote working in terms of resource availability and employee preparedness. Most employees had little or no time to adjust to new remote working routines, with most hoping that the new working conditions would only be temporary [5], [6]. Unfortunately, that was never the case in most scenarios, especially after organizations experienced the benefits of remote working. The speedy adoption of remote working due to the pandemic never laid a proper foundation for remote working infrastructure and workforce preparedness.

Several companies launched the work-from-home (WFH) initiative when the pandemic peaked. In the United States, 17% of the working population worked from home before COVID-19, compared to almost 50% during the pandemic [4]. Also, Hackney et al. [4] posited that nearly 40% of Europe's workforce engaged in WFH arrangements during the pandemic compared to 10%

during COVID-19 [4]. In Australia, WFH arrangements increased from less than 20% to about 50% within months of the pandemic's spread [4]. Most likely, the increased adoption of WFH initiatives and its current prevalence may have never been possible without the COVID-19 spike. Still, several managers are glad that remote working helped improve productivity, primarily IoT, due to efficient use of time and increased resource access. The pandemic considerably changed employee norms regarding the work environment [6], [7]. Ongoing digital transformation working setups, both physical and virtual, will keep prompting employees to keep an open mind on working practices and nurture new perspectives.

B. Prevalence of IoT Monitoring in the Organization

Technology is part of daily living, considering the everyday use of smartphones and other electronic devices like computers. For more than a decade now, IoT has been a megatrend, fueling Industry 4.0 so that just about any object, regardless of size and role, can be connected and managed remotely [8]. Factors like technological advancements, which ease IoT implementation, and reduced costs of sensors foster the increasing implementation of IoT solutions in remote working [9]. Also, millennials dominate the global workforce, with many open to technology-driven solutions like remote working and IoT [6]. The ease of device interconnectivity and remote monitoring through IoT-based technologies enables ongoing process management and personnel surveillance opportunities. IoT monitoring is possible across all industries globally, as it is practical to embed any device with sensors and transform physical objects into smart objects. Dahlqvist et al. [9] revealed that the number of IoT adoption in business settings increased from 13% in 2014 to 25% in 2019, with a projected increase in the future. Sievers et al. [10] also recorded an accelerating growth of IoT adoption in business settings, necessitating real-time monitoring of associated devices and applications. Consistent monitoring allows predictive maintenance for better system efficiency.

As a valuable commodity instrumental in making informed choices, information flows seamlessly through interconnected systems (machine-to-machine (M2M) interaction) between machines and humans (human-to-human (H2H) interaction), letting people navigate problems easily [11]. Continued technological advancements have transformed how businesses operate by improving efficiency and allowing the completion of tasks within short time frames. Also, real-time monitoring quickly shapes how companies conduct business by keeping track of time-critical functions. Technical innovations facilitate mass production through process automation, improving production scale while minimizing production costs [1]. Through IoT monitoring, managers can achieve the full potential of technical solutions. The IoT monitoring concept has been around for several years, but its widespread adoption became a critical concern with the rise of the COVID-19 pandemic, which promoted remote working. This implies a significant relationship between IoT monitoring and remote working.

Besides the pandemic-imposed remote working, organizations now have remote working arrangements, giving employees an option to work from home or allowing employees to choose their preferred working routes. According to Sievers et al. [10], remote working enables employees to access all organizational resources (based on authorization) on personal dashboards without support. On the other hand, Sengupta and Al-Khalifa [6] maintained that remote work's impact varies depending on whether it is mandatory or optional. When employees opt for the WFH arrangement, they may receive less support and access to organizational resources than when the company makes a section of its workers work from home [6]. As a mandatory WFH rule, the company will meet all the fundamental employee needs to maximize efficiency. Those opting to work remotely at will may attract suspicion and resentment among co-workers [6]. As employees keep experiencing new working conditions and exposure to innovative solutions, their acceptance of remote working as associated technologies like IoT monitoring will improve.

C. Sustainable Approaches

Waste reduction refers to eliminating redundant business of system processes, while cost reduction is minimizing production, operational, and maintenance costs. However, supply chain redundancy is essential in lean production techniques as it promotes resilience under risky environments [12]. Kamalahmadi et al. [12] defined redundancy as "practices in which a firm takes action in advance of a disruption, incurring the cost of the action regardless of whether a disruption occurs." It

supports lean operations by avoiding wasting money, time, and effort in the event of system breakdown through IoT-driven management. IoT monitoring tracks performance to optimize operations by discovering and assessing connected devices. Through IoT monitoring, analysts can eliminate inefficient processes before they further compromise business productivity, reducing operating and maintenance costs [13]. The underlying sustainable benefit involves cost savings by predicting consumption and spending that guarantee improved profitability in the long run [14]. For example, through real-time surveillance and predictive analytics, managers can determine possible outcomes based on a specific line of investment to increase the likelihood of success.

Monitoring and managing the workflow of raw materials in supply chain management have long-lasting benefits to an organization. Radio Frequency Identification (RFID) has sensory wireless networks and relies on IoT monitoring for ubiquitous data access to identify materials through an Internet connection for real-time information feeds [2], [14]. That way, it is easy to identify, locate, and provide necessary resources in time at the proper location, enhancing process efficiency. Also, RFID-IoT technology limits human errors, serving as cost-effective means of supply chain management. In turn, improved accuracy in operations performance within the organization's supply chain reduces turnover rates while increasing employee satisfaction levels [14], [15]. Also, IoT-embedded sensors for tracking products minimize operation processes while showing managers the current process completion or fulfillment rates of employee tasks [15]. IoT is a tracking asset because RFID sensors help employees locate lost devices [13]. Upon recognizing how IoT monitoring helps them become competent workers, employees are more likely to embrace the technology in remote working. Further, Sievers et al. [10] argued that IoT monitoring improves employee job satisfaction as IoT solutions prevent employees from being overwhelmed. The workforce feels the company is trying to increase productivity by reducing workload.

The sustainability of IoT monitoring in remote working business structures involves optimal cloud usage, which refers to the potential environmental benefits of green cloud computing to society [13], [14]. Companies adopting remote working rely on cloud solutions, including cloud servers, storage, and applications, to conduct business operations. Cloud computing offers real-time resource and process management through automation. Centralized data collection, analysis, resource management, and process surveillance through cloud platforms reduce waste due to shared resources [14]. The most fundamental components of cloud computing to reduce costs are pay-as-you-go and on-demand characteristics [16]. These features ensure that users spend on the exact quantity of resources used. For example, when setting up on-premise storage, an organization may purchase 500 terabytes and never use the whole volume – the unused space goes to waste. IoT integration with cloud solutions connects enterprise systems with cloud data centers, reducing energy consumption by limiting the power used to run on-premise servers and machines [13]. This is the basis of the green cloud, which allows organizations to share cloud resources through virtual infrastructures to minimize costs and reduce carbon footprint. Also, cloud computing securely and automatically configures IoT devices for monitoring business practices. Self-configuration of cloud-based IoT devices requires standard and interoperable protocols [13]. Finally, remote working allows employees and managers to manage their time effectively.

D. Ethical Considerations

Remote working is not a one-size-fits-all arrangement [4]. Employees in one company may be open to IoT monitoring, but others in a different company may be completely uncomfortable with the ideas. Sometimes, IoT monitoring depends on the company's cultural perspectives regarding technology acceptance and how workers feel about their privacy and confidentiality [5], [17]. Managers should determine whether employees feel safe and willing to expose their private information in a collaborative workspace, knowing that colleagues and supervisors can use the information to assess their competence. Metwally et al. [5] posited that an individual's readiness to change significantly influences organizational change. The determinants of change include contexts, such as corporate leadership and cultural views; content, such as the need and extent of change; and process, such as employee experience in preceding change attempts [5]. People are more likely to change under good leadership

that acknowledges unique employee needs and preferences. For example, when deriving business policies for IoT monitoring, it is essential to engage the workforce. The portrayal of commitment through transformational leadership makes employees comfortable with their leaders' prepositions on IoT monitoring [5], [18]. However, forcing change without consulting employees triggers resistance, often leading to failed interventions.

IoT technology enables data tracking in a remote working setting with shared resources. The applied process is an antecedent of change based on employee response to previous projects [5]. Assessing the factors that led to past failures and resistance to adopting a specific digital solution in the organization can create room for different approaches. Informed employees are often wary of data tracking vulnerabilities following IoT deployment [17]. If the organization has sufficient data about its workforce, it can use practical approaches for IoT monitoring by leveraging the unique preferences of workers. Princi and Krämer [17] linked the acceptance of IoT monitoring among workers to the amount of tracked data, how much the employee trusts their employer and the perceived benefits of IoT surveillance systems. The deployment of smart technology may cause mistrust, significantly lowering employee commitment [17]. Trust may go both ways; the employee may not trust the system and the employers, making it even harder for the solution to succeed. The best way to build trust among workers is to make them feel valued and engaged in decision-making [19], [20]. Employees who trust their leaders will likely overlook the possible challenges, including ethical drawbacks, of IoT monitoring in remote working.

Further, employees are more likely to comply with new organizational changes surrounding IoT monitoring if they can trust their leaders than if they feel their privacy is at risk. Tradeoffs between employee privacy and open data access limit successful regulatory frameworks [5], [21]. Ethical issues emerge in organizational settings when companies collect, store, and use employee data with minimal transparency and accountability [5]. IoT surveillance raises privacy and confidentiality concerns as some employees are uncomfortable sharing their private data with the company. Even when a company protects employee data and values their privacy, it is worth addressing the underlying risks surrounding data security in case of information misuse and data breaches [21]. Accordingly, firms should outline data access and usage policies aligning with industry regulations. However, establishing appropriate industry standards and regulations that fully support IoT monitoring in remote working settings may take years, considering misaligned technical, social, and political priorities.

The perceived benefits of IoT surveillance align with the need for adoption [5], [17]. Organizations sometimes adopt innovative solutions primarily because they fall into emerging technologies. Just because a technology is new does not mean it is worth implementing. It is better to prioritize functionality than newness to avoid integration issues considering most employees are resistant to change [5]. The ethical considerations surrounding IoT monitoring in remote working involve overlooking employee skillsets by reducing them to executors from decision-makers. Sievers et al. [10] averred that IoT monitoring overtakes routine employee practices through process automation, making employees believe that artificial intelligence (AI) is threatening their job security. AI technologies in IoT systems responsible for data analytics mimic human intelligence. If employees feel like they will lose their job to smart machines, they question IoT's essence in their lives. At this point, IoT's need for adoption seems like a strategy to replace workers so that the workforce lacks autonomy and empowerment [10]. Employees who feel they have no control over their work domains or extensively interact with technology develop negative attitudes towards digital transformations, hindering IoT implementation [10], [17], [22]. IoT monitoring in remote working should not threaten employees' perceived value but instead. IoT should exhibit mild disruptions, especially when managers introduce the workforce to the associated innovations.

Implementing IoT monitoring should not dwell entirely on organizational productivity but also consider employee willingness to comply. IoT devices collect massive user data, sometimes without users willing to share their data [5], [20]. For example, a corporate laptop assigned to an employee for remote working can be configured to collect employee data automatically without the user's consent or, sometimes, knowledge.

Also, some devices lack effective security parameters, risking employees' privacy and physical safety and undermining employee trust [17], [20]. Allhoff and Henschke [20] stipulated, "There have been a series of cases where smart devices have been sent data picked up by cameras and microphones from people's homes back to the producer's servers for analysis, without clear or obvious consent from the users." IoT devices potentially violate user privacy and transmit data without informed consent, taking advantage of the fact that most users have little knowledge about their technical workings. An organizational IoT device and information system should consider the moral values of employees beyond data security. Limited employee knowledge of how organizations secretly collect private data makes them vulnerable to privacy and confidentiality risks.

Finally, some studies have linked remote working to perceived autonomy [3]. A significant number of the modern workforce prefer remote working over on-premise working due to flexibility and taking control over one's working schedule without having to deal with annoying supervisors. The underlying concern is whether such employees are willing to trade their privacy under unregulated IoT monitoring conditions for convenience. Stills it worth acknowledging that not all employees are well informed on the risks surrounding digital surveillance facilitated by IoT-enabled devices [20]. Still, it is troubling how some employees have little regard for their privacy by sharing personal data through digital platforms.

III. Conclusion

The COVID-19 pandemic accelerated remote working, increasing WFH arrangements globally; this presented managers with an excellent opportunity to explore the benefits of remote working through IoT surveillance to operate sustainably. The increased adoption of remote working permit IoT monitoring as organizations find it beneficial to assess business functions for improved productivity. A sustainable approach towards IoT monitoring in remote working emerges as businesses eliminate redundant processes and unnecessary management costs. Some factors impeding successful IoT monitoring involve limited employee trust in smart technology and their leaders and the perceived benefits, which compromise IoT acceptance. The ethical dynamics compromising IoT solutions in remote working primarily involve employee privacy and safety since employees fear the risk of open access to personal data. Unfortunately, some people lack sufficient knowledge of the adversities of IoT monitoring, increasing their risk of data threats. However, continued exposure to IoT monitoring in remote working may speed up adoption.

References

[1] J. Nagy, J. Oláh, E. Erdei, D. Máté, and J. Popp, "The Role and Impact of Industry 4.0 and the Internet of Things on the Business Strategy of the Value Chain—The Case of Hungary," *Sustainability*, vol. 10, no. 10, p. 3491, Sep. 2018, doi: 10.3390/su10103491.

[2] A. M. Rahmani, S. Bayramov, and B. Kiani Kalejahi, "Internet of Things Applications: Opportunities and Threats," *Wirel. Pers. Commun.*, vol. 122, no. 1, pp. 451–476, Jan. 2022, doi: 10.1007/s11277-021-08907-0.

[3] B. Wang, Y. Liu, J. Qian, and S. K. Parker, "Achieving Effective Remote Working During the COVID‐19 Pandemic: A Work Design Perspective," *Appl. Psychol.*, vol. 70, no. 1, pp. 16–59, Jan. 2021, doi: 10.1111/apps.12290.

[4] A. Hackney, M. Yung, K. G. Somasundram, B. Nowrouzi-Kia, J. Oakman, and A. Yazdani, "Working in the digital economy: A systematic review of the impact of work from home arrangements on personal and organizational performance and productivity," *PLoS One*, vol. 17, no. 10 October, 2022, doi: 10.1371/journal.pone.0274728.

[5] D. Metwally, P. Ruiz-Palomino, M. Metwally, and L. Gartzia, "How Ethical Leadership Shapes Employees' Readiness to Change: The Mediating Role of an Organizational Culture of Effectiveness," *Front. Psychol.*, vol. 10, Nov. 2019, doi: 10.3389/fpsyg.2019.02493.

[6] D. Sengupta and D. Al-Khalifa, "Pandemic Imposed Remote Work Arrangements and Resultant Work-Life Integration, Future of Work and Role of Leaders—A Qualitative Study of Indian Millennial Workers," *Adm. Sci.*, vol. 12, no. 4, p. 162, Nov. 2022, doi: 10.3390/admsci12040162.

[7] R. F. Guzzo, X. Wang, J. M. Madera, and J.

Abbott, "Organizational trust in times of COVID-19: Hospitality employees' affective responses to managers' communication," *Int. J. Hosp. Manag.*, vol. 93, p. 102778, Feb. 2021, doi: 10.1016/j.ijhm.2020.102778.

[8] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of Things (IoT): A Review of Its Enabling Technologies in Healthcare Applications, Standards Protocols, Security, and Market Opportunities," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10474–10498, Jul. 2021, doi: 10.1109/JIOT.2021.3062630.

[9] F. Dahlqvist, M. Patel, A. Rajko, and J. Shulman, "Growing opportunities in the Internet of Things," *McKinsey & Company*, 2019. https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things (accessed Jan. 20, 2023).

[10] F. Sievers, H. Reil, M. Rimbeck, J. Stumpf-Wollersheim, and M. Leyer, "Empowering employees in industrial organizations with IoT in their daily operations," *Comput. Ind.*, vol. 129, p. 103445, Aug. 2021, doi: 10.1016/j.compind.2021.103445.

[11] A. Ometov *et al.*, "A Survey on Wearable Technology: History, State-of-the-Art and Current Challenges," *Comput. Networks*, vol. 193, p. 108074, Jul. 2021, doi: 10.1016/j.comnet.2021.108074.

[12] M. Kamalahmadi, M. Shekarian, and M. Mellat Parast, "The impact of flexibility and redundancy on improving supply chain resilience to disruptions," *Int. J. Prod. Res.*, vol. 60, no. 6, pp. 1992–2020, Mar. 2022, doi: 10.1080/00207543.2021.1883759.

[13] S. Tripathi and L. Pandit, "Analysis of Factors Influencing Adoption of Internet of Things: A System Dynamics Approach," *Theor. Econ. Lett.*, vol. 09, no. 07, pp. 2606–2625, 2019, doi: 10.4236/tel.2019.97164.

[14] W. C. Tan and M. S. Sidhu, "Review of RFID and IoT integration in supply chain management," *Oper. Res. Perspect.*, vol. 9, p. 100229, 2022, doi: 10.1016/j.orp.2022.100229.

[15] M. M. Miah, "The impact of employee job satisfaction toward organizational performance: A study of private sector employees in Kuching, East Malaysia," *Int. J. Sci. Res. Publ.*, vol. 8, no. 12, pp. 270–278, Dec. 2018, doi: 10.29322/IJSRP.8.12.2018.p8437.

[16] R. Ara, M. A. Rahim, S. Roy, and D. U. K. Prodhan, "Cloud computing: Architecture, services, deployment models, storage, benefits and challenges," *Int. J. Trend Sci. Res. Dev.*, vol. 4, no. 4, pp. 837–842, 2020.

[17] E. Princi and N. C. Krämer, "Acceptance of Smart Electronic Monitoring at Work as a Result of a Privacy Calculus Decision," *Informatics*, vol. 6, no. 3, p. 40, Sep. 2019, doi: 10.3390/informatics6030040.

[18] H. Liu, "A brief analysis of learning organization practice from the perspective of the fifth discipline model theories—A case study of Jatco (Guangzhou)," *Am. J. Ind. Bus. Manag.*, vol. 08, no. 11, pp. 2143–2157, 2018, doi: 10.4236/ajibm.2018.811142.

[19] V. Verma, "Employee's Participation in Decision Making Process," *Int. J. Res. Sci. Innov.*, vol. IV, no. VI, pp. 118–121, 2017.

[20] F. Allhoff and A. Henschke, "The Internet of Things: Foundational ethical issues," *Internet of Things*, vol. 1–2, pp. 55–66, Sep. 2018, doi: 10.1016/j.iot.2018.08.005.

[21] J. Scheibner, A. Jobin, and E. Vayena, "Ethical Issues with Using Internet of Things Devices in Citizen Science Research: A Scoping Review," *Front. Environ. Sci.*, vol. 9, Feb. 2021, doi: 10.3389/fenvs.2021.629649.

[22] E. Marsh, E. P. Vallejos, and A. Spence, "The digital workplace and its dark side: An integrative review," *Comput. Human Behav.*, vol. 128, p. 107118, Mar. 2022, doi: 10.1016/j.chb.2021.107118.