The Effectiveness of IoT Based Wearable Devices and Potential Cybersecurity Risks: A Systematic Literature Review from the Last Decade

https://doi.org/10.3991/ijoe.v18i09.32255

Mohd Fazli Mohd Sam[1](✉), Albert Feisal Muhd Feisal Ismail[1], Kamarudin Abu Bakar[1], Amiruddin Ahamat[1], Muhammad Imran Qureshi[2]
[1]Faculty of Technology Management and Technopreneurship, Universiti Teknikal Malaysia (UTeM), Melaka, Malaysia
[2]Teesside University International Business School, Teesside University, Middlesbrough, United Kingdom
mohd.fazli@utem.edu.my

Abstract—Wearable technology has enormous promise, particularly for data collection for cutting-edge health research, and its popularity has soared in recent years. This study aims to provide IoT-based wearable devices' effectiveness and potential cybersecurity threats to these innovative technologies. Using the PRISMA-2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology, we conducted a scoping study to understand better the application of inexpensive, consumer-grade wearables for health research from a population health viewpoint. Scopus databases yielded a total of 43 articles. Our findings show that academics and research participants are tremendously interested in this technology, but they are also wary about using wearables. These devices are still vulnerable to cybersecurity assaults such as data privacy and security in healthcare. However, blockchain technology is a potential alternative for integrating with IoT-based wearables to ensure data privacy. Furthermore, according to the findings, wearables have an increasingly diverse range of applications, including COVID-19 prediction, fertility tracking, heat-related sickness, pharmacological effects, and psychological therapies; they also include underrepresented populations, such as those with rare diseases. In low-resource environments, there is a lack of research on wearable devices.

Keywords—wearable devices, IoT, cybersecurity, smart applications, blockchains, healthcare

1 Introduction

Over the last decade, there has been a surge in consumer devices for measuring health and fitness. Wearable technology is expected to grow from 325 million linked devices in 2016 to 929 million devices in 2021 [1]. Wearable technology revolutions have uncovered exciting biomedical and health care technologies [2]. In addition, wearable devices are a significant ubiquitous Internet of Things technology in everyday life. Effective

data processing in different devices such as bright clothing, smartwatches, smart wristwear, medical wearables, and consumer-oriented services of IoT technology is unavoidable [3]. The wearable market is now dominated by health, safety, interaction, tracking, identification, fitness, and similar applications. Wearables facilitate the merging of the physical and digital worlds, bringing individuals into the IoT [4]. Wearable devices flip the traditional paradigm of health care delivery, with users initiating data gathering and health questions rather than clinicians [5]. One of the primary beneficiaries of wearable technology in healthcare is monitoring patients and tracking their behaviours [6].

In recent years, the healthcare sector has become increasingly reliant on wearables, and COVID-19 was a watershed moment in the advancement of IoT-based wearables [7]. Wearable gadgets safeguard healthcare staff from the viral transmission and monitor affected patients during the saviour pandemic [8]. In addition, wearable gadgets have evolved as a new technology that plays a vital role in continuous health monitoring. These devices can measure physiological characteristics, including heart rate and arterial blood pressure, human mobility and everyday activities [9]. Most health records are sent through IoT-based wearable devices to healthcare record centres for additional processing and decision making [10]. However, many academics are voicing concerns about the privacy and security of data collected by wearable devices and health care facilities [11], [12]. According to [13], security threats can typically be external risks such as hackers, viruses, and worms are often classified as external threats, whereas interior threats such as unintentional data loss are classified as internal threats.

Although wearable devices have the potential to improve individual health and monitoring, cyber security problems are associated with IoT-based wearables [14]. According to [15], internet-connected sensors, equipment, and networks are frequently the focus of cyberattacks, extortion, theft, and even destruction. Because an IoT-based smart grid might include millions of online nodes spread across vast geographical areas, it is the most vulnerable to severe cyberattacks. A cyber-strike would thus have terrible consequences and significant financial damage because such an assault would bring entire countries to a standstill. Additionally, healthcare wearable devices include patients' critical data and possible cyber security concerns. However, the researchers ignored the literature's relationship between wearable technologies and cyber security. There is a substantial disconnect between IoT-enabled wearable devices and potential cyber security risks. Quite a few studies and academics have explored the significance of this sector, and it is very noteworthy because the number of users is increasing daily.

The current research investigates the significance of wearable devices and possible cyber security risks to this cutting-edge technology. The current study also analyzed the effectiveness of wearable devices in the healthcare sector. Additionally, the present study will discover potential cyber security physical systems to safeguard users' data. The current study employed the PRISMA statement 2020 to include and exclude data from the Scopus database to achieve the study's purpose.

2 Research methodology

For assessing existing research, this article used the PRISMA (Preferred Reporting Items for Systematic Review and Meta-Analysis Protocols) framework 2020 [16].

The scoping method was utilized following the PRISMA standards to acquire the most relevant material on "wearable devices AND cyber security" possible research keywords. They broadened the scope of wearable technologies and cybersecurity issues, conducting a thorough literature analysis utilizing the Scopus database to locate relevant scientific papers and articles. Multiple keywords grouping searches were carried out to collect relevant published literature from the most prestigious and trustworthy research database—the term wearable devices utilized in the Scopus database to search the relevant literature. The document search was enhanced by implementing preset quality requirements from the PRISMA declaration 2020inclusion and exclusion criteria. The following part will go through the inclusion and exclusion method about quality criteria. The absence of a publishing timetable characterizes the literature pursuit. Initially, 69 documents were shown. The review subjects include computer science, engineering, business management, and medical; the findings are restricted to 66; nevertheless, this included all sorts of records, such as research articles, reviews, and conference papers, and 55 papers were picked. The final literature hunting resulted in 43 records from the Scopus database. The records were then transferred to an Excel sheet to carry on a further systematic review process. The PRISMA statement 2020 framework execution in this review is shown in Figure 1.

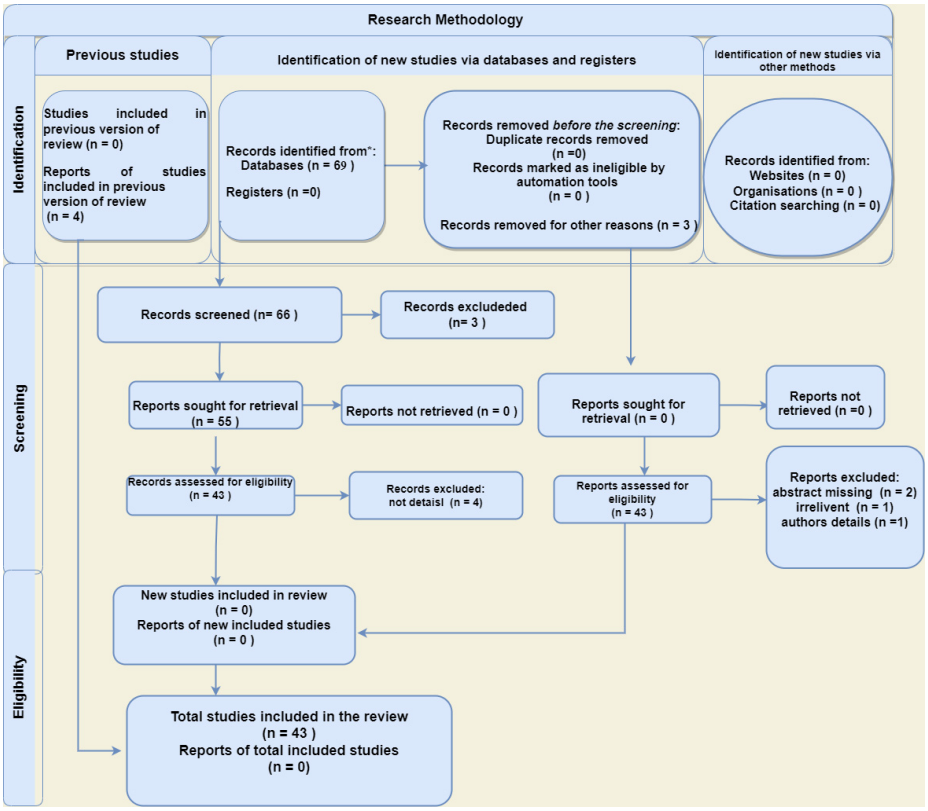

Fig. 1. PRISMA statement 2020 inclusion and exclusion criteria

2.1 Quality evaluation

This study examines published articles and review papers to identify the most accepted findings and indicate the published research. The results, abstracts, and conclusions were separated to limit the number of entries. It also considered referenced references in the evaluated publications. The records were often checked to avoid duplication and improve the needed findings; extraneous research was also removed.

2.2 Eligibility and inclusion articles

The following inclusion and exclusion criteria were used for the selected research articles: Examine articles in the English language to ensure proper selection. In addition, papers were indicated whether they were published in the Scopus database. This article examines the literature on wearable technologies and cybersecurity threats, identifies previous research, and discusses prospects for digital technology.

2.3 Studies included in qualitative synthesis

Following the selection of the papers, two procedures were taken to guarantee the quality of the analysis was performed on the selected documents. Initially, Microsoft Excel entered the trustworthy information to study the wearable technologies literature, such as the segments and settings. Comprehensive content analysis is conducted to identify and monitor significant examination streams, write recent research across several areas, and flag potential difficulties and possibilities for further study. Using a content analysis approach and subsequent texts, classify and grade the apparent statement content concerning intended groups using an organized strategy, permitting reproducible and valid text proposals.

2.4 Descriptive

We utilised the subjects' criteria to choose appropriate articles for the review from the database. The database included computer science, engineering, medicine, business management, and accounting. Computer science made the most significant contribution, accounting for 32% of all records. The other notable findings came from engineering, with 26% of the publications. Figure 2 depicts the detailed results of the subject selection criteria.

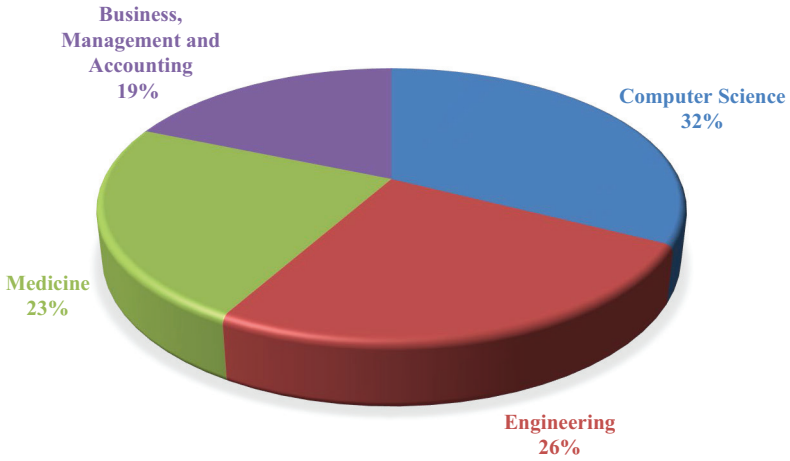

Fig. 2. Distribution of subjects

Additionally, the year of publishing is depicted in Figure 3. Wearable devices have been developed significantly in recent years, and scholars have contributed important scholarly work [17]. In the current research, 2021 provides 15 publications, and the other significant number was reported in 2020, with 11 records. The years 2019, 2018, 2017, and 2016 provided 4, 2, 4 and 3 articles.

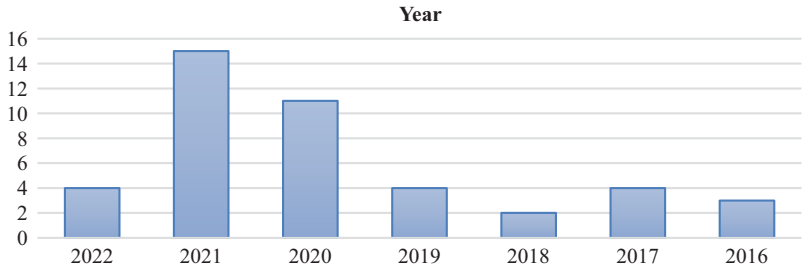

Fig. 3. Distribution of year base publication

Furthermore, the sources of the retrieved records are an essential aspect of the current investigation. With eight papers, Advances in Intelligent Systems and Computing had the highest number of published records, and IEE Access supplied seven records, while IEEE Internet Of Things Journal contributed the same number of records. Other significant numbers are drawn from Studies in Health Technology and Informatics and Lecture Notes in Computer Science, Including Subseries, which contain 5, 6 papers each. The distribution of sources is seen in Figure 4 below.

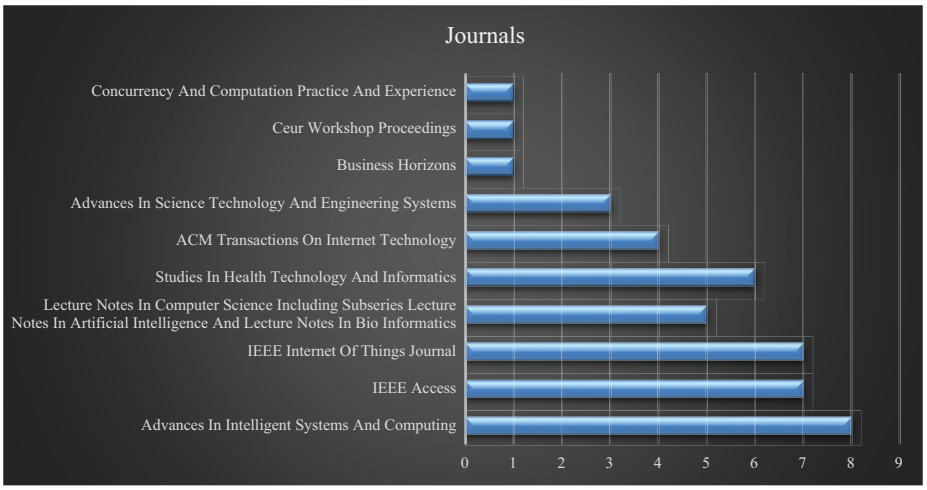

Fig. 4. Distribution of articles extracted from the sources

2.5 Literature mapping

Additional categorization of literature leads to the published literature and researcher view on wearable devices and cybersecurity in healthcare. We used the keywords wearable devices, IoT, cybersecurity, cyber-physical systems, and privacy to studies contained in the keywords in literature review phase 1; these records were also used to recognize the literature classifications from these keywords, as Table 1 shows. The table explains four three major classifications occurrence with terms, occurrences, and relevance scores of each key term. Each term is a minimum of 4 times used in the selected literature and a maximum of 12 times. The key terms occurrences are divided into categories of cyber security, IoT, and wearable devices. Table 1 depicts the details of actual term occurrences.

Table 1. Critical term occurrences analysis

Classification	Term	Occurrences	Relevance Score
Cyber security systems	adoption	6	0.6729
	attack	11	0.587
	attacker	5	1.1758
	blockchain	4	0.6547
	cybersecurity attack	4	1.1552
	data privacy	4	1.7094
	impact	7	0.9916
	problem	9	1.058
	requirement	4	1.0691
	safety	4	1.225
	solution	5	0.4339
	threat	8	1.4129
	world	4	0.9263
IoTs	article	7	0.4278
	artificial intelligence	6	2.173
	big data	4	2.4719
	development	9	0.9134
	implementation	4	0.3322
	infrastructure	6	0.6627
	iot	12	0.4771
	IoT device	7	1.2691
	number	8	1.4403
	person	6	0.7438
	recent year	4	1.751
	storage	4	0.6989
	study	9	1.3767
	term	4	0.4966

(Continued)

Table 1. Critical term occurrences analysis *(Continued)*

Classification	Term	Occurrences	Relevance Score
Wearable devices	access	6	1.3294
	daily life	5	0.665
	effectiveness	5	1.1504
	evidence	6	1.9998
	framework	12	0.715
	integration	6	1.326
	life	5	0.8397
	mobile device	5	0.6477
	opportunity	7	0.7221
	patient	12	0.8881
	sensor	12	0.5741
	set	5	1.0434
	smartphone	8	0.2979
	usability	5	0.877
	use	7	0.7876
	wearable	6	0.8303

The documents were additionally examined via content analysis to determine the classifications of the study. VOSViewer software analyzes the published literature' content—data clusters created on the text established to group the related ideas. The current study formed that researchers' keywords and keywords in more detail in the journals' indexing procedure outlined in the databases are equally accurate for bibliometric analysis designed to uncover the structures of the examining field. Hence, we involved both classes of keywords for the co-occurrence analysis within the study area associated with wearable devices. In total, 43 records were contained within the research. We have thoroughly established and selected only the most numerous 43 keywords repetitive a minimum of 4 times. Figure 4 illustrates the content analysis results—the group showed four large clusters, described in different colours in Figure 5. The cluster is represented by orange displays yellow to illustrate cyber security, effectiveness, and IoT devices. The cluster in blue is primarily ascribed to mobile devices and smartphones. The green cluster signifies implementation, data privacy sensors, IoTs and patients. Ultimately, the purple cluster indicates cryptocurrencies and peer-to-peer. Each cluster is further examined in the next section to determine wearable devices and cybersecurity.

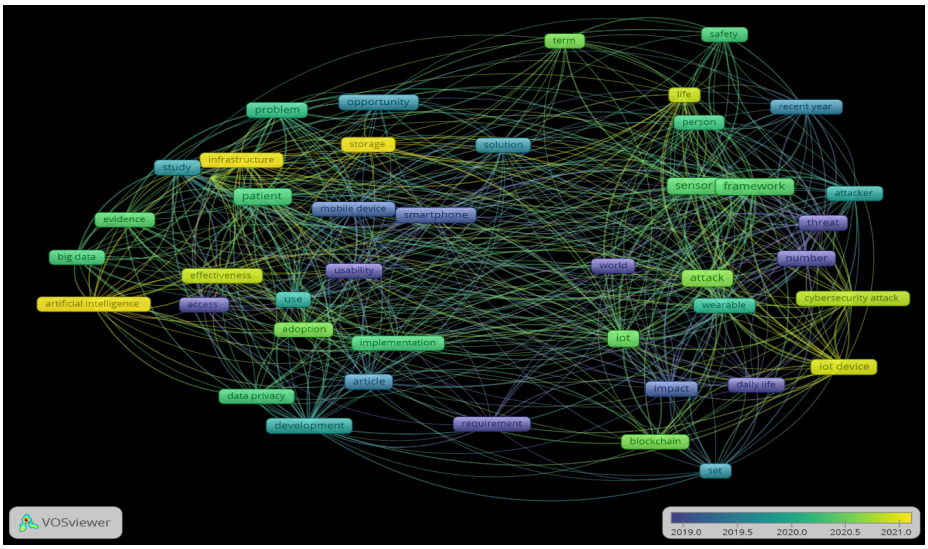

Fig. 5. Content analysis to identify the classifications

3 Classification

3.1 Internet of things (IoT)

The convergence of several technologies, such as wireless technologies, microelectromechanical systems (MEMS), microservices, and the Internet, has aided in creating IoT [18]. The use of these various technologies resulted in the convergence of operational technologies (OT) and information technologies (IT), permitting the creation of systems capable of collecting data from the environment and exchanging it over the Internet [19]. IoT devices must be safeguarded, but so must their communications: massive amounts of data can be transmitted between devices and between the latter and servers or customers, and compromising the availability, integrity, or confidentiality of this data might have serious consequences [20]. According to [21], the Internet of Things (IoT) has dominated Internet usage since its introduction into our daily lives in numerous forms, such as home appliances and wearable gadgets. This prevailing behaviour has left network practitioners with several problems with IoT devices, including development, deployment, security, privacy, and ethics. Considering that the data created and received by IoT devices contains a substantial quantity of personal data, processing, storing, and protecting data protection of information acquired from IoT devices is a critical problem that must not be overlooked [22]. Table 2 below illustrated the details of authors contributed on IoTs in current study.

Table 2. Distribution of authors, year, citations, settings, and segments

Authors	Year	Cited by	Settings	Segment
Zendehdel G.A., Kaur R., Chopra I., Stakhanova N., Scheme E.	2022		wearable health	cyberattacks
Melchor-Uceda I.A., Olivares-Rojas J.C., Gutiérrez-Gnecchi J.A., García-Ramírez M.C., Reyes-Archundia E., Téllez-Anguiano A.C.	2021		health sector	storage
Bouchaud F., Vantroys T., Grimaud G.	2021		wearable devices	legal and forensic sense
Canbaz M.A., O'Hearon K., McKee M., Hossain M.N.	2021		wearable devices	security, privacy, and ethics
Upman V., Goranin N.	2020	1	wearable wellness devices	cybersecurity
Roldán J., Boubeta-Puig J., Luis Martínez J., Ortiz G.	2020	38	smartphones and wearables	cybersecurity attacks and threats
Fournier H., Kondratova I., Molyneaux H.	2020	1	Older adults	wearables and emerging intelligent systems
Singh D., Tripathi G., Shah S.C., Da Rosa Righi R.	2018	5	Internet of Vehicle (IoV)	wearable, sensors, smartphones
Langone M., Setola R., Lopez J.	2017	8	healthcare scenario	wearable device
Williams M., Axon L., Nurse J.R.C., Creese S.	2016	6	future technologies	security and privacy

Moreover, because of naive designs and inadequate security implementations, wearable devices have been and continue to be vulnerable to cyberattacks. Worryingly, the security of wearable medical gadgets is considerably worse. When these susceptible devices are connected to networks, they expose whole digital healthcare infrastructures to security risks, and pervasive internet access significantly expands the attack surface [23]. According to [24], cybersecurity is a critical component of a secure, effective, and dependable healthcare delivery system. Security and privacy issues may be resolved by following best practices to protect systems and devices. Wearables and home IoTs pose substantial privacy threats. In addition, IoT is empowering as a new generation technology, and IoT security considerations are crucial. Many researchers suggested various machine learning and neural network approaches to construct improved anomaly-based IoT intrusion detection systems with high accuracy, yet these proposed systems appear to be vulnerable to cyberattacks [25]. Finally, cybersecurity frameworks must work together to address the security problems associated with IoT devices and implement preventative tactics and algorithms to avoid these possible hazards.

3.2 Wearable devices and innovative technologies

Innovative technological advances are reshaping the research, development, and delivery of health goods and services and drastically altering how diseases are diagnosed, treated and avoided. The applicability of wearable devices and mobile

applications is increasing in healthcare perspectives, making patient monitoring and comprehension of daily behaviours more straightforward than before [26]. According to [27], the usage of intelligent technologies speeds up clinical studies. Smart gadgets may speed up clinical research by collecting data in real-time, resulting in enhanced data collection compliance and quality improvement. In addition, today's smartphones come pre-installed with health-related apps and sensors capable of measuring vital physiological parameters such as oxygen saturation [28].

Additionally, wearable and implanted medical gadgets are increasingly used to diagnose, monitor, and treat severe medical problems. Medical equipment like these are instances of safety-critical, cyber-physical systems [29]. According to [30], digital health solutions can enhance the lives of diabetics and other related diseases, and wearable monitoring is a crucial element in this regard. Aside from that, wearable gadgets are rapidly infiltrating various healthcare clinical processes in hospitals, necessitating the skills of physicians and nurses to address the skill gap in this field [31]. Table 3 shows the authors contributed the wearable devices and innovative technologies.

Table 3. Distribution of authors, year, citations, settings, and segments

Authors	Year	Cited by	Settings	Segment
Manyazewal T., Woldeamanuel Y., Blumberg H.M., Fekadu A., Marconi V.C.	2021	9	Digital Health	capacity require
Panda A., Pinisetty S., Roop P.	2021		medical devices	cyber-physical systems
Maccioni G., Giansanti D.	2021	2	medical apps	cybersecurity
Gomez G., Espina E., Armas-Aguirre J., Molina J.M.M.	2021		Internet of Things	cybersecurity
Baumann A.P., O'Neill C., Owens M.C., Weber S.C., Sivan S., D'Amico R., Carmody S., Bini S., Sawyer A.J., Lotz J.C., Goel V., Dmitriev A.E.	2021	1	traditional orthopaedic devices	cybersecurity, and regulatory considerations
Kooman J.P., Wieringa F.P., Han M., Chaudhuri S., Van Der Sande F.M., Usvyat L.A., Kotanko P.	2020	11	Digitization of healthcare	wearable health
Alharbi A., Alharbi T.	2020	2	smartphones	Authentication Framework for Wearable Devices
Nguyen T., Gosine R.G., Warrian P.	2020	30	big data	cybersecurity
Klonoff D.C., Kerr D., Wong J.C., Pavlovic Y., Koliwad S., Hu J., Salber P., Aguilera A., Long W., Hamilton G., Chen K.Y., Adi S.	2017	1	Diabetes Technology	patients in selecting treatment
Ehrler F., Blondon K., Baillon-Bigotte D., Lovis C.	2017	6	electronic health record	authentication management
Mills A.J., Watson R.T., Pitt L., Kietzmann J.	2016	19	laptops and tablets	wearable device

Mobile applications enable users of smartphones and wearable devices to monitor their behaviour, which reduces the number of patients seeking healthcare [32]. The makers and users of commercially accessible wearable devices that monitor and report personal health-related data such as physical activity and vital signs in real-time will drive a significant portion of this revolution rather than healthcare practitioners. Miniaturization of electronics is a critical enabler for wearable health devices [33]. However, wearable devices are a new technology that needs authentication methods because, while they may be thought of as extensions of mobile devices (e.g., smartphones), their form factors are fundamentally different. People use mobile devices in a "bursty" manner, which indicates that they are often utilised for brief periods [34]. However, security is crucial in all information systems; the nature of the security problem in the case of wearable devices is sufficiently different to merit specific consideration [35]. First and foremost, wearables are by far the most personalised computing devices. While the settings may change significantly, it is simple for one individual to use another's desktop or laptop computer [36].

3.3 Cyber security

Industry 5.0 refers to the industrial procedure's automation, digitalization, and data transmission, which includes industrial cyber-physical systems (I-CPSs), industrial Internet of Things (IIoT), and artificial intelligence (AI). Intelligent wearable devices have been widely used in the healthcare environment to detect body information and monitor patients' health conditions [37]. According to [38], a cyber-physical system (CPS) is defined as "engineered systems that are developed from and rely on the tight integration of computer algorithms and physical elements" and serves as the foundation of the fourth industrial revolution. In addition, most linked systems, known as Cyber-Physical Systems (CPS), are built by combining several elements such as humans and the physical environment, intelligent objects, and embedded devices and infrastructure [39]. A few significant difficulties might harm the IoT and CPS, such as security vulnerabilities and ethical concerns [40]. Cybersecurity in the context of wearable devices has received much attention. Many academics are concentrating on integrating blockchain technology with IoT-based wearable gadgets to reduce cyber security risks [41], [42]. One of blockchain technology's innovative features is its ability to create decentralised architecture for formerly centralised services [43]. Table 4 illustrates the details of the cybersecurity authors' contribution.

Table 4. Distribution of authors, year, citations, settings, and segments

Authors	Year	Cited by	Settings	Segment
Ramasamy L.K., Khan F., Shah M., Prasad B.V.V.S., Iwendi C., Biamba C.	2022		Internet of Things (IoT	security risks and ethical issues
Do Y., Hoang L.T., Park J.W., Abowd G.D., Das S.	2021		cybersecurity warnings	smartwatches
Chinaei M.H., Habibi Gharakheili H., Sivaraman V.	2021	1	wearable sensors	Internet-of-Things (IoT) sensors
Vlasenko A.V., Putyato M.M., Makaryan A.S.	2021		Biometric	Internet of things
Nguyen T., Gosine R.G., Warrian P.	2021		personal health monitoring	COVID-19
Javid T., Faris M., Beenish H., Fahad M.	2020	3	Health Industry 4.0	cyber-physical systems
Quasim M.T., Algarni F., Radwan A.A.E., Alshmrani G.M.M.	2020	7	healthcare systems	security, privacy and efficiency
Narikimilli N.R.S., Kumar A., Antu A.D., Xie B.	2020	2	digital transformation in health	Blockchain
Koppel R., Kuziemsky C.	2019	1	cyber-criminals	financial and personal data

Blockchain, a tamper-proof database, provides unique possibilities for addressing many concerns linked to the IoT ecosystem's security and privacy [44]. Researchers highlighted security and privacy issues for IoT applications at several tiers of the protocol stack in a recent and assessed blockchain-based solution established by previous works for scalable access management, trust, safe storage, authentication, and access control [45]. According to [46], blockchain technology has the potential to relieve the healthcare industry of these burdens by establishing a blockchain of medical records. Because of its digital encryption, blockchain is believed to be highly secure, transparent, and resilient to hackers. It also plays a vital role in minimising intermediary costs because it is decentralised. In addition, to keep the patient's data safe against unwanted access. A blockchain framework is incredibly secure against unauthorised access or misuse. Appropriate for preserving confidence between various parties and stakeholders [47]. The use of blockchain technology is a critical component in ensuring the data security and privacy of those who use wearable devices. The healthcare industry throughout the world is migrating IoT-based wearables and electronic records to blockchains to safeguard hospitals' crucial information [48].

4 Conclusion

Wearables can substantially influence the general health and well-being of people of various ages, genders, and ethnicities. Most significantly, wearables have the potential to promote health equality by enhancing access to timely care and treatment across racial, socioeconomic, and geographical boundaries [49]. The current study examined

the effectiveness of wearable devices and possible cybersecurity risks to data transfer in healthcare systems. According to the findings, researchers recognize the importance of IoT-based wearable devices such as smartwatches, sensors, wearable ECG monitors, wearable blood pressure monitors, and wearable biosensors in healthcare [50]. Over time, healthcare professionals and academics found these revolutionary technologies in healthcare, and advanced technologies are integrating infrastructure with these wearables owing to consumer desire on a wide scale in recent years [51]. The growth of the IoT in healthcare is no longer a secret for the industry and researchers. Current study findings indicate that releasing numerous new wearable goods daily that integrate healthcare applications such as health apps, ECG, blood pressure monitoring, and stress level assessment through wearable devices.

However, many researchers' findings show that cybersecurity vulnerabilities are present in these wearable devices, and much effort needs to be made to enhance data security and privacy problems [52]. Aside from that, blockchain technologies are growing in the healthcare sector to provide data privacy and electronic record security. The data security during data transmission from wearable devices and sensors must be safe and secure by utilising blockchain technology. The integration of IoTs based wearable devices and blockchain still need more interest in future research.

5 Acknowledgements

This work was supported by the Short Term Research Grant from Universiti Teknikal Malaysia Melaka under Grant No: PJP/2020/FPTT/PP/S01766.

6 References

[1] A. Banerjee, C. Chakraborty, A. Kumar, and D. Biswas, "Emerging trends in IoT and big data analytics for biomedical and health care technologies," *Handbook of Data Science Approaches for Biomedical Engineering*, pp. 121–152, Jan. 2020, https://doi.org/10.1016/B978-0-12-818318-2.00005-2

[2] C. C. Cheung, A. D. Krahn, and J. G. Andrade, "The emerging role of wearable technologies in detection of arrhythmia," *Canadian Journal of Cardiology*, vol. 34, no. 8, pp. 1083–1087, Aug. 2018, https://doi.org/10.1016/j.cjca.2018.05.003

[3] M. S. Patel, D. A. Asch, and K. G. Volpp, "Wearable devices as facilitators, not drivers, of health behavior change," *JAMA – Journal of the American Medical Association*, vol. 313, no. 5. pp. 459–460, 2015. https://doi.org/10.1001/jama.2014.14781

[4] J. J. Ferreira, C. I. Fernandes, H. G. Rammal, and P. M. Veiga, "Wearable technology and consumer interaction: a systematic review and research agenda," *Computers in Human Behavior*, vol. 118, p. 106710, May 2021, https://doi.org/10.1016/j.chb.2021.106710

[5] Z. Gao and J. E. Lee, "Emerging technology in promoting physical activity and health: challenges and opportunities," *Journal of Clinical Medicine*, vol. 8, no. 11, p. 1830, Nov. 1, 2019. https://doi.org/10.3390/jcm8111830

[6] K. I. Jang *et al.*, "Self-assembled three dimensional network designs for soft electronics," *Nature Communications*, vol. 8, Jun. 2017. https://doi.org/10.1038/ncomms15894

[7] M. Ndiaye, S. S. Oyewobi, A. M. Abu-Mahfouz, G. P. Hancke, A. M. Kurien, and K. Djouani, "IoT in the wake of Covid-19: a survey on contributions, challenges and evolution," *IEEE Access*, vol. 8, pp. 186821–186839, 2020. https://doi.org/10.1109/ACCESS.2020.3030090

[8] M. Tavakoli, J. Carriere, and A. Torabi, "Robotics, smart wearable technologies, and autonomous intelligent systems for healthcare during the COVID-19 pandemic: an analysis of the state of the art and future vision," *Advanced Intelligent Systems*, vol. 2, no. 7, p. 2000071, Jul. 2020, https://doi.org/10.1002/aisy.202000071

[9] P. K. Beh, Y. Ganesan, M. Iranmanesh, and B. Foroughi, "Using smartwatches for fitness and health monitoring: the UTAUT2 combined with threat appraisal as moderators," *Behaviour and Information Technology*, vol. 40, no. 3, pp. 282–299, 2021, https://doi.org/10.1080/0144929X.2019.1685597

[10] K. Hameed, I. S. Bajwa, S. Ramzan, W. Anwar, and A. Khan, "An intelligent IoT based healthcare system using fuzzy neural networks," *Scientific Programming*, vol. 2020, 2020, https://doi.org/10.1155/2020/8836927

[11] R. Basatneh, B. Najafi, and D. G. Armstrong, "Health sensors, smart home devices, and the internet of medical things: an opportunity for dramatic improvement in care for the lower extremity complications of diabetes," *Journal of Diabetes Science and Technology*, vol. 12, no. 3, pp. 577–586, May 2018, https://doi.org/10.1177/1932296818768618

[12] H. Sikandar, Y. Vaicondam, N. Khan, M. I. Qureshi, and A. Ullah, "Scientific mapping of industry 4.0 research: a bibliometric analysis," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 18, 2021. https://doi.org/10.3991/ijim.v15i18.25535

[13] L. Cilliers, "Wearable devices in healthcare: privacy and information security issues," *Health Information Management Journal*, vol. 49, no. 2–3, pp. 150–156, May 2020, https://doi.org/10.1177/1833358319851684

[14] N. Khan and M. I. Qureshi, "A systematic literature review on online medical services in Malaysia," *International journal of online and biomedical engineering*, vol. 16, no. 6, pp. 107–118, 2020, https://doi.org/10.3991/ijoe.v16i06.13573

[15] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 36–49, Jun. 2019, https://doi.org/10.1016/j.ijcip.2019.01.001

[16] H. Y. Park, C. H. Suh, S. Woo, P. H. Kim, and K. W. Kim, "Quality reporting of systematic review and meta-analysis according to PRISMA 2020 guidelines: results from recently published papers in the Korean journal of radiology," *Korean Journal of Radiology*, vol. 23, no. 3, pp. 355–369, Mar. 2022, https://doi.org/10.3348/kjr.2021.0808

[17] S. El-Gebali *et al.*, "The Pfam protein families database in 2019," *Nucleic Acids Research*, vol. 47, no. D1, pp. D427–D432, Jan. 2019, https://doi.org/10.1093/nar/gky995

[18] M. Langone, R. Setola, and J. Lopez, "Cybersecurity of wearable devices: an experimental analysis and a vulnerability assessment method," *Proceedings – International Computer Software and Applications Conference*, vol. 2, pp. 304–309, Sep. 2017, https://doi.org/10.1109/COMPSAC.2017.96

[19] I. A. Melchor-Uceda, J. C. Olivares-Rojas, J. A. Gutiérrez-Gnecchi, M. C. García-Ramírez, E. Reyes-Archundia, and A. C. Téllez-Anguiano, "Data ingestion system for interoperability and integration of hospital data online and in real time," *2021 Mexican International Conference on Computer Science, ENC 2021*, Aug. 2021, https://doi.org/10.1109/ENC53357.2021.9534795

[20] J. Roldán, J. Boubeta-Puig, J. Luis Martínez, and G. Ortiz, "Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks," *Expert Systems with Applications*, vol. 149, p. 113251, Jul. 2020, https://doi.org/10.1016/j.eswa.2020.113251

[21] M. A. Canbaz, K. J. O'Hearon, M. McKee, and M. N. Hossain, "IoT Privacy and Security in Teaching Institutions: Inside The Classroom and Beyond," 2021.

[22] F. Bouchaud, T. Vantroys, and G. Grimaud, "Forensic analysis of IoT ecosystem," in *Proceedings – 2021 International Conference on Future Internet of Things and Cloud, FiCloud 2021*, Aug. 2021, pp. 115–122. https://doi.org/10.1109/FiCloud49777.2021.00024

[23] D. Singh, G. Tripathi, S. C. Shah, and R. Da Rosa Righi, "Cyber physical surveillance system for Internet of Vehicles," in *IEEE World Forum on Internet of Things, WF-IoT 2018 – Proceedings*, May 2018, vol. 2018, pp. 546–551. https://doi.org/10.1109/WF-IoT.2018.8355218

[24] H. Fournier, I. Kondratova, and H. Molyneaux, "Designing digital technologies and safeguards for improving activities and well-being for aging in place," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2020, vol. 12426 LNCS, pp. 524–537. https://doi.org/10.1007/978-3-030-60149-2_40

[25] L. Wang and C. A. Alexander, "Big data analytics in medical engineering and healthcare: methods, advances and challenges," *Journal of Medical Engineering and Technology*, vol. 44, no. 6, pp. 267–283, Aug. 17, 2020. https://doi.org/10.1080/03091902.2020.1769758

[26] G. Gomez, E. Espina, J. Armas-Aguirre, and J. M. M. Molina, "Cybersecurity architecture functional model for cyber risk reduction in IoT based wearable devices," 2021. https://doi.org/10.1109/CONIITI53815.2021.9619624

[27] A. P. Baumann *et al.*, "FDA public workshop: orthopaedic sensing, measuring, and advanced reporting technology (SMART) devices," *Journal of Orthopaedic Research*, vol. 39, no. 1, Ltd, pp. 22–29, Jan. 01, 2021. https://doi.org/10.1002/jor.24833

[28] G. Maccioni and D. Giansanti, "Medical apps and the gray zone in the covid-19 era: between evidence and new needs for cybersecurity expansion," *Healthcare (Switzerland)*, vol. 9, no. 4, p. 430, Apr. 2021, https://doi.org/10.3390/healthcare9040430

[29] A. Panda, S. Pinisetty, and P. Roop, "A secure insulin infusion system using verification monitors," in *Proceedings of the 19th ACM-IEEE International Conference on Formal Methods and Models for System Design, MEMOCODE 2021*, 2021, pp. 56–65. https://doi.org/10.1145/3487212.3487342

[30] D. C. Klonoff *et al.*, "Digital diabetes congress 2017," *Journal of Diabetes Science and Technology*, vol. 11, no. 5, pp. 1045–1052, Sep. 2017, https://doi.org/10.1177/1932296817723037

[31] S. Soderi, "Cybersecurity assessment of the polar bluetooth low energy heart-rate sensor," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 2019, vol. 297 LNICST, pp. 252–265. https://doi.org/10.1007/978-3-030-34833-5_20

[32] T. Manyazewal, Y. Woldeamanuel, H. M. Blumberg, A. Fekadu, and V. C. Marconi, "The potential use of digital health technologies in the African context: a systematic review of evidence from Ethiopia," *npj Digital Medicine*, vol. 4, no. 1, pp. 1–13, Aug. 17, 2021. https://doi.org/10.1038/s41746-021-00487-4

[33] J. P. Kooman *et al.*, "Wearable health devices and personal area networks: Can they improve outcomes in haemodialysis patients?" *Nephrology Dialysis Transplantation*, vol. 35, no. Supplement_2, pp. II43–II50, Mar. 01, 2020. https://doi.org/10.1093/ndt/gfaa015

[34] A. Alharbi and T. Alharbi, "Design and evaluation of an authentication framework for wearable devices," *IEEE Access*, vol. 8, pp. 80369–80381, 2020. https://doi.org/10.1109/ACCESS.2020.2990861

[35] A. J. Mills, R. T. Watson, L. Pitt, and J. Kietzmann, "Wearing safe: physical and informational security in the age of the wearable device," *Business Horizons*, vol. 59, no. 6, pp. 615–622, Nov. 2016, https://doi.org/10.1016/j.bushor.2016.08.003

[36] F. Ehrler, K. Blondon, D. Baillon-Bigotte, and C. Lovis, "Smartphones to access to patient data in hospital settings: Authentication solutions for shared devices," in *Studies in Health Technology and Informatics*, 2017, vol. 237, pp. 73–78. https://doi.org/10.3233/978-1-61499-761-0-73

[37] S. Shamshad *et al.*, "An efficient privacy-preserving authenticated key establishment protocol for health monitoring in industrial cyber–physical systems," *IEEE Internet of Things Journal*, vol. 9, no. 7, pp. 5142–5149, Aug. 2021, https://doi.org/10.1109/JIOT.2021.3108668

[38] T. Javid, M. Faris, H. Beenish, and M. Fahad, "Cybersecurity and data privacy in the cloudlet for preliminary healthcare big data analytics," *2020 International Conference on Computing and Information Technology, ICCIT 2020*, Sep. 2020, https://doi.org/10.1109/ICCIT-144147971.2020.9213712

[39] R. Koppel and C. Kuziemsky, "Healthcare data are remarkably vulnerable to hacking: connected healthcare delivery increases the risks," *Studies in Health Technology and Informatics*, vol. 257, pp. 218–222, 2019, https://doi.org/10.3233/978-1-61499-951-5-218

[40] L. K. Ramasamy, F. Khan, M. Shah, B. V. V. S. Prasad, C. Iwendi, and C. Biamba, "Secure smart wearable computing through artificial intelligence-enabled internet of things and cyber-physical systems for health monitoring," *Sensors*, vol. 22, no. 3, p. 1076, Jan. 2022, https://doi.org/10.3390/s22031076

[41] A. Vlasenko, M. Putyato, A. M.-P. of the V, and undefined 2020, "Possibilities of improving the cyber security of mobile devices based on the integration of dynamic biometric methods," *ceur-ws.org*, 2021.

[42] M. I. Qureshi, N. Khan, H. Raza, A. Imran, and F. Ismail, "Digital technologies in education 4.0. Does it enhance the effectiveness of learning? A systematic literature review," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 4, 2021. https://doi.org/10.3991/ijim.v15i04.20291

[43] M. H. Chinaei, H. Habibi Gharakheili, and V. Sivaraman, "Optimal witnessing of healthcare IoT data using blockchain logging contract," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 10117–10130, Jun. 2021, https://doi.org/10.1109/JIOT.2021.3051433

[44] T. Nguyen, R. G. Gosine, and P. Warrian, "Digitalization of the oil and gas industry: practical lessons learned from digital responses during the first stage of the COVID-19 outbreak," in *Advances in Intelligent Systems and Computing*, 2021, vol. 1290, pp. 313–325. https://doi.org/10.1007/978-3-030-63092-8_21

[45] A. Vlasenko, M. Putyato, A. M.-P. of the V, and undefined 2020, "Possibilities of improving the cyber security of mobile devices based on the integration of dynamic biometric methods," *ceur-ws.org*, 2021.

[46] N. R. S. Narikimilli, A. Kumar, A. D. Antu, and B. Xie, "Blockchain applications in healthcare – a review and future perspective," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2020, vol. 12404 LNCS, pp. 198–218. https://doi.org/10.1007/978-3-030-59638-5_14

[47] M. T. Quasim, F. Algarni, A. A. E. Radwan, and G. M. M. Alshmrani, "A blockchain based secured healthcare framework," in *2020 International Conference on Computational Performance Evaluation, ComPE 2020*, Jul. 2020, pp. 386–391. https://doi.org/10.1109/ComPE49325.2020.9200024

[48] S. Mekruksavanich and A. Jitpattanakul, "Convolutional neural network and data augmentation for behavioral-based biometric user identification," in *Advances in Intelligent Systems and Computing*, 2021, vol. 1270, pp. 753–761. https://doi.org/10.1007/978-981-15-8289-9_72

[49] S. J. Woodruff, P. Coyne, and E. St-Pierre, "Stress, physical activity, and screen-related sedentary behaviour within the first month of the COVID-19 pandemic," *Applied Psychology: Health and Well-Being*, vol. 13, no. 2, pp. 454–468, May 2021. https://doi.org/10.1111/aphw.12261

[50] S. D. Mamdiwar, R. Akshith, Z. Shakruwala, U. Chadha, K. Srinivasan, and C. Y. Chang, "Recent advances on iot-assisted wearable sensor systems for healthcare monitoring," *Biosensors*, vol. 11, no. 10, p. 372, Oct. 04, 2021. https://doi.org/10.3390/bios11100372

[51] J. J. Ferreira, C. I. Fernandes, H. G. Rammal, and P. M. Veiga, "Wearable technology and consumer interaction: A systematic review and research agenda," *Computers in Human Behavior*, vol. 118, p. 106710, May 2021, https://doi.org/10.1016/j.chb.2021.106710

[52] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: threats and potential solutions," *Computer Networks*, vol. 169, p. 107094, Mar. 2020, https://doi.org/10.1016/j.comnet.2019.107094

7 Authors

Mohd Fazli Mohd Sam, Faculty of Technology Management and Technopreneurship, Universiti Teknikal Malaysia (UTeM), Melaka, Malaysia. E-mail: mohd.fazli@utem.edu.my

Albert Feisal Muhd Feisal Ismail, Faculty of Technology Management and Technopreneurship, Universiti Teknikal Malaysia (UTeM), Melaka, Malaysia. E-mail: feisal@utem.edu.my

Kamarudin Abu Bakar, Faculty of Technology Management and Technopreneurship, Universiti Teknikal Malaysia (UTeM), Melaka, Malaysia. E-mail: kamarudin@utem.edu.my

Amiruddin Ahamat, Faculty of Technology Management and Technopreneurship, Universiti Teknikal Malaysia (UTeM), Melaka, Malaysia. E-mail: amiruddin@utem.edu.my

Muhammad Imran Qureshi, Teesside University International Business School, Teesside University, Middlesbrough, United Kingdom. E-mail: m.qureshi@tees.ac.uk

Article submitted 2022-05-06. Resubmitted 2022-06-22. Final acceptance 2022-06-24. Final version published as submitted by the authors.