Received: 7 June 2022 | Revised: 16 August 2022 | Accepted: 7 September 2022

DOI: 10.1002/hsr2.863

ORIGINAL RESEARCH

Health Science Reports Open Access WILEY

Internet of Things and healthcare system: A systematic review of ethical issues

Somayyeh Zakerabasali[1] | Seyed Mohammad Ayyoubzadeh[2]

[1]Department of Health Information Management, Clinical Education Research Center, Health Human Resources Research Center, School of Health Management and Information Sciences, Shiraz University of Medical Sciences, Shiraz, Iran

[2]Department of Health Information Management, School of Allied Medical Sciences, Tehran University of Medical Sciences, Tehran, Iran

Correspondence
Somayyeh Zakerabasali, Department of Health Information Management, Health Human Resources Research Center, Shiraz University of Medical Sciences, Shiraz 14336-71348, Iran.
Email: zakerabasi@gmail.com

Abstract

Background and Aims: The Internet of Things (IoTs) is a set of connected objects and devices that share data and pursue a common goal in different areas. IoT technology can significantly help the healthcare system by enabling the monitoring of elderly and chronic disease patients. Along with the growth of this technology, its challenges and limitations such as Connectivity, Compatibility, Standards, cost, legal, and ethical also increase. One of the most critical and challenging issues in the IoT is ethical issues. This study aims to explore the key ethical aspects of the IoT and Categorize them based on the executive phases of IoT in healthcare.

Methods: The current study was conducted in two phases using the mixed-method approach. In the first phase, a systematic review was conducted in relevant databases to identify ethical issues of the IoT. In the second phase, a focus group discussion was conducted to classify the extracted data elements based on executive phases of IoT by medical informatics experts and computer engineerings.

Results: Among the 138 papers retrieved through the search strategy, 11 articles were selected, and 12 ethical issues related to IoT were identified. The obtained results revealed the importance of ethical issues of IoT, including security, confidentiality, privacy, anonymity, freedom to withdraw, informed consent, integrity, availability, authorization, access control, censoring, and eavesdropping. They were classified into five main categories of executive phases of IoT based on the five experts' opinions affiliated with SUMS, including data collection, data storage, data process, data transmission, and data delivery.

Conclusion: Because of the key role of the IoT in disease prevention, real-time tele-monitoring of patient's functions, testing of treatments, health management, and health research, considering the risks relating to Health care and patient data is essential. Moreover, health policymakers should be aware of the ethical commitment to using IoT technology.

KEYWORDS

ethical issues, healthcare, Internet of Things, IoT

1 | INTRODUCTION

The Internet of Things (IoT) provides the concept of the smart world that things will be able to interact with other things by connecting to the Internet or with the help of communication tools and sharing their information with each other or humans. IoT provides new classes of capabilities, applications, and services to help people. It will be a world in which all things and heterogeneous devices will be able to have addresses and controllability.[1] The IoT will be considered a future innovation in wireless technologies and will be applied in many areas. It is defined from different perspectives.[2] For instance, from the viewpoint of[3]:

1. Services provided by things: is "the world in which all things can automatically communicate with computers and provide all services for the benefit of humans."[4]
2. Connection: is "the ability to communicate with anyone or anything at any time or in any place."[5]
3. Communications: "an extensive network of interconnected objects with unique addresses based on standard communication protocols."[6]
4. Networks: is "an internet developed from a network of interconnected computers to a network of interconnected objects."[7]

One of the important applications of the IoT in various medical areas is remote patient monitoring systems and emergency alert systems, and follow-up of discharged patients. Since monitoring the health parameters of patients is done through sensors on their bodies, IoT may allow patients to stay in various places, such as their homes, workplaces, public places, or vehicles, while medical sensors are still attached to them and transferring information to the medical center.[8] Health care systems can provide many advantages of IoT, such as the patient with chronic diseases monitoring, monitoring the elderly, and receiving quick medical responses from physicians. As a result of this, hospital costs will be dramatically reduced through immediate intervention and quick treatment.[2,9] The main goal of IoT in the electronic health system is to help current healthcare monitoring systems through real-time and online monitoring of vital signs and health data for the patient. In this approach, complete and precise data transfer from patients to medical centers is essential.[10] Failure to do this might jeopardize the patient's life. One of the existing challenges in the area of modern technological tools is related to the issue of ethics. The aim of this study is to discuss ethical concepts of executive phases of IoT in healthcare.

2 | METHODS

The methodology applied here is that of a mixed-method approach. A systematic review and expert consensus were used to retrieve relevant ethical issues. We adhered to the protocol to review articles based on preferred items to report in systematic reviews and meta-analyses (PRISMA).[11] The current study was conducted in two phases:

2.1 | Phase 1: Identification of the ethical issues in IoT technology using the systematic review

In the first phase of this study, a systematic review was conducted in relevant databases, including PubMed, Scopus, and Web of Science, to identify appropriate ethical issues of IoT technology. Keywords that were used to search for sources of information include words related to the concepts of "internet of things" and "Ethics". The search string is defined as follows: (("internet of things" OR "IoT") AND ("Ethic*")). Articles that were published between 2013 and 2022 were selected. Our inclusion criteria were: full-text papers with the relevant keywords in the title or abstracts, studies that were published from 2013 to February 2022, and studies published in the English language. In addition, review and systematic review articles were included in the search result, and articles that did not report any ethical issues were excluded. In the first step, the abstract and title of articles were studied according to the inclusion/exclusion criteria. Screening of titles and abstracts was conducted independently by two researchers. The disagreement between researchers was resolved by consensus. In the next step, The full texts of articles, which seemed relevant to the objectives, were reviewed by the same two researchers. Any disagreement was resolved by consensus. Finally, ethical issues were extracted from the selected articles.

2.2 | Phase 2: Classification of the ethical issues using the focus group discussion

During the first phase of the research, the identified ethical issues employed various classifications of the data elements. Therefore, a focus group discussion was used to classify the extracted ethical issues based on executive phases of IoT in healthcare by contributing five experts affiliated with SUMS (three medical informatics and two computer engineering). They were selected due to their familiarity with IoT technology and experience in the field of medical sciences. To adhere to ethical considerations, the experts participated in the study with full knowledge of the objective of the research and could withdraw from the study at any time. This focus group was held in the department of health information management at Shiraz University of medical science. This session lasted 2 h. All extracted ethical issues were discussed with all experts' opinions taken into account.

2.3 | IoT system executive phases

IoT has five phases based on online and offline requests. These phases include collecting data to delivering data.

1. Data collection: The first step is gathering, collecting, or receiving data from devices and objects. Different data collectors based on the characteristics of objects are used. The object might be a fixed object like body sensors or radio-frequency identification (RFID) tags or a dynamic and moving device like sensors and chips.
2. Data storage: Data collected from the previous phase should be stored. If the object has an internal memory, the data can be stored. Typically, IoT components are installed with low memories and low processing powers. Clouds will take responsibility for storing data when devices' internal memory is unavailable.
3. Data process: IoT analyzes the data stored in the data center of the clouds and provides smart services for work and life in real-time. In addition, IoT not only analyzes and responds to queries but also controls objects. IoT provides smart processing and controls the services of all objects identically.
4. Data transmission: Data transmission occurs in all stages: from sensors, RFID tags, or chips to data centers, from data centers to process units, processors to controllers, devices, and end-users.
5. Data delivery: Delivering the processed data to objects at the moment without any errors or changes is an essential and sensitive task that should always be done.[12,13]

3 | RESULTS

3.1 | Phase 1

Based on the search strategy, a total of 138 articles were retrieved. Overall, there were 23 duplicates among the databases, which were excluded. After removing duplicates, the abstract and title of 115 articles were studied. At this stage, 80 articles were excluded, considering the irrelevance of the article title or abstract. The full texts of 35 articles seemed relevant to the objectives. In the final analysis, 11 articles were selected, and 12 ethical issues related to IoT were identified. The literature search results are shown in Figure 1, and the result of extracted ethical issues from these 12 articles are presented in Table 1.

3.2 | Phase 2

Based on the experts' opinions, the ethical issues were assigned into five main categories: data collection, storage, process, data transmission, and delivery. The major categories of IoT ethical issues are summarized in Figure 2. Data collection included five elements: confidentiality, security, anonymity, freedom to withdraw, and informed consent. Data storage includes five elements: security, confidentiality, integrity, authorization, and availability. Censoring is the only item of the data process. Data transmission includes authorization, integrity, confidentiality, availability, anonymity, access control, and eavesdropping. And finally, Data delivery included two elements: confidentiality and access control.

4 | DISCUSSION

The IoT has made great strides in recent years in all areas, especially in healthcare, which has attracted the attention of many researchers and developers worldwide. This technology, despite its advantages, has many challenges that can lead to failure or being useless. One of the most important and challenging issues in the IoT is ethical issues. Therefore, the identification of each of these issues and their solutions in accordance with the implementation phases of this technology should be considered. The categories and items obtained in the findings are discussed as follows.

4.1 | Data collection

One of the most important issues in this area is collecting and exchanging individuals' data with information technology. Today, many individuals are hired to collect, explore and distribute data. This large size of private information can threaten ethical issues. For example, violation of individuals' privacy is one of these challenges. Most people's information may be used for various purposes without their awareness of individuals.[24,25]

1. Confidentiality: Protecting the confidentiality of the collected data in an online study requires techniques and measures that are quite different from protecting the confidentiality of paper-based data. Using secure sockets layers (SSL) when the data are sent to servers makes data transmission secure. Security equipment, such as encryption, can be useful measures for protecting the data on the server. Online collected data will probably be as secure as locked and protected data in research laboratories with such safety measures.[26]
2. Data security: Confidential data and information collected from participants should be safely stored, protected, and eliminated. This can be achieved through passwords, physical locks, and limiting the staff who can access the identified data.
3. Anonymity: Identifying information needs to show the consent and agreement of individuals, presenting contact information for receiving data or payment, and allocating credit for participation in research should be kept in a place separate from the data collected from that study. For instance, these data can be kept in a separate database. Therefore, in case an error occurs or data are available to individuals without permission, the data will be at least anonymous.
4. Freedom to withdraw: Freedom for participants and samples taking part in medical research should be preserved. Participants should have completely clear and obvious information on who, for what purpose, and to what extent they should have access to their data to decide to provide their data for research applications.[26]
5. Informed consent: During online data collection, researchers might never meet the participants, which suggests a challenge in informed consent. Informed consent is one of the most

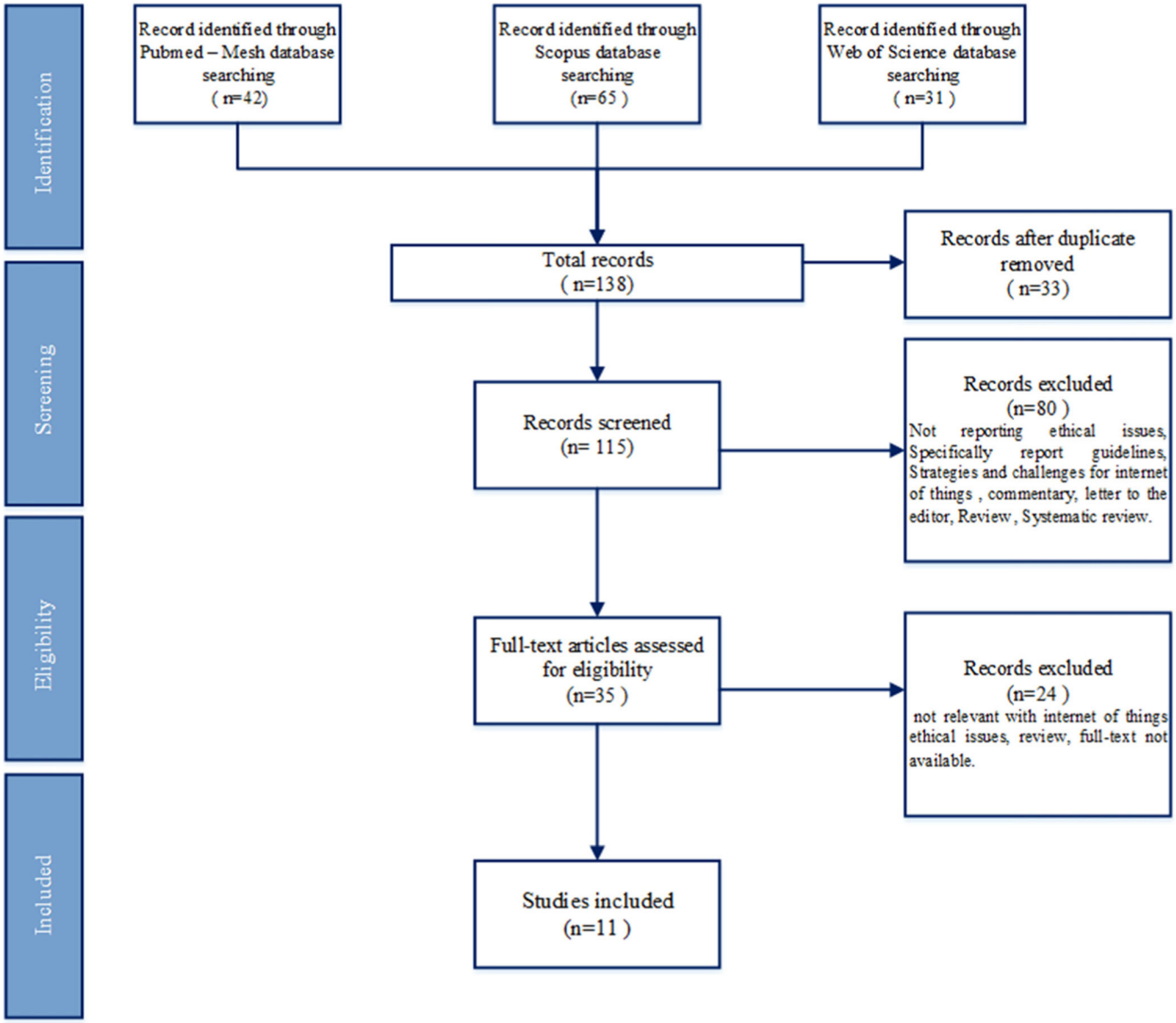

FIGURE 1 PRISMA flow diagram with the steps in the article selection process. PRISMA, preferred items to report in systematic reviews and meta-analyses.

fundamental concepts in medical ethics and patient rights in the world, such that acquiring informed consent before any diagnostic and therapeutic activity will have positive ethical and clinical results. Informed consent is considered a major component of patient rights in healthcare centers. It is a process in which the patient or their legal representative understands and agrees to the treatment plan.[27]

4.2 | Data storage

In the data storage process, data protection and security are considered major factors for acquiring the trust of users and successful use of cloud computing.[28] Cloud computing has changed the environment. Right now, people are transferring their information to clouds, particularly since data have grown larger and they need more devices to be accessible. Therefore, data security and confidentiality have always been important issues in information technology.[16] And in this situation, data security in cloud computing is becoming more and more important.[29,30]

1. Data security: Data security covers four main areas: Encryption, server security, client security, and password security.
   - Encryption: One of the major components of security is encryption. SSL is an industrial encryption technology that provides online banking security and electronic commerce. SSL guarantees all communications between your computer and cloud-based servers.
   - Server security: While SSL helps establish safe communication between your computer and a cloud, you also need to make

TABLE 1 Result of extracted ethical issues from selected articles in the field of the Internet of Things

Study	Security	Confidentiality	Privacy	Anonymity	Freedom to withdraw	Informed consent	Integrity	Availability	Authorization	Access control	Censoring	Eavesdropping
Chang et al.[14]	*	*	*	*	*	*	*	*	*	*	*	*
El-Khoury & Arikan[15]	*	*	*	*		*	*	*		*		
Baldini et al.[16]	*		*	*	*	*		*	*	*		
Karale[17]	*	*	*	*		*	*	*	*	*	*	*
Philip et al.[18]	*	*	*	*		*	*	*	*			
Aledhari et al.[19]	*		*			*	*	*	*	*		*
Olawole[20]	*	*	*					*		*		*
Nadian-Ghomsheh et al.[21]	*	*	*					*		*		
Lhotska et al.[22]	*	*	*	*		*			*	*		
Popescul & Georgescu[10]	*	*	*			*	*		*	*		
Furstenau et al.[23]	*		*	*			*	*	*	*		

sure that servers are safe against hackers and other threats. Although it is pretty difficult to assess the security of cloud-based servers for web users, there are services by companies that regularly assess security on SaaS providers to ensure the security of servers.

- Client security: Although cloud computing has the advantage of outsourcing server-level security and backup, an overlooked part of the security equation is the security of the desktop or laptop from which you are accessing the SaaS application.
- Password security: Finally, security also encompasses password security. The best SSL encryption and client/server security can be undone by choice of a weak password. Thus, care should be given when choosing a password.[31,32]

2. Data confidentiality: Data confidentiality is very important for users to store their private or confidential data. Strategies for identification and access control are used to ensure data confidentiality. In general, all information you enter into a cloud computing application should be considered confidential and private information that cannot be used by the cloud computing provider. Furthermore, the cloud computing provider should only be permitted to view any of your private information with your explicit consent (e.g., to troubleshoot a technical issue).
3. Data integrity: Data integrity is one of the most important factors in all information systems. In general, data integrity means the protection of data against unauthorized elimination, change, or construction. Data integrity is a basis for offering cloud computing services such as SaaS, PaaS, and IaaS. In addition to storing data on a large scale, cloud computing generally provides data processing services. Such techniques can achieve data integrity as redundant array independent disks strategies and digital signatures.
4. Authorization: Authorization is used for data access control. It is a mechanism by which a system determines the level of access by valid users for working with secure sources under the control of the system.[33,34]
5. Availability: Companies needing to store large-scale data have two options: Using a local data center or storing with a cloud. If appropriately used, storing in a cloud enables such companies to use resources in various geographical regions to ensure data availability even when they face local/regional/district disasters.[35–37]

4.3 | Data process

Cloud computing has two essential processes: (1) Data processing and computing, and (2) Data storing. In the data processing and computing process, users of cloud services do not need anything, and they can have access to their data and fulfill their computing and processing tasks only through a connection to the Internet. Clients do not even know where the data are stored during data availability and computing and what device or machine carries out the task of computing.[13,32]

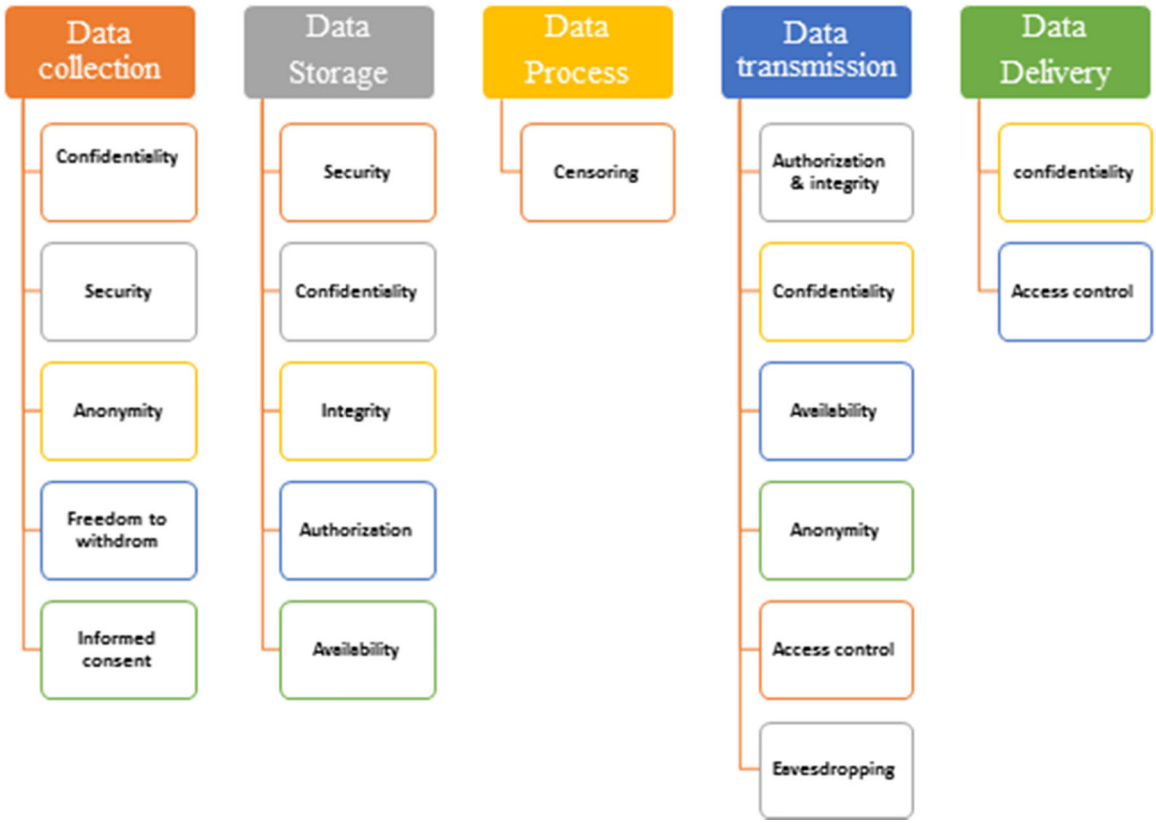

FIGURE 2 Ethical issues based on executive phases of IoT system. IoT, Internet of Things.

1. Censoring: Censoring data and findings is an important ethical issue. Censoring can occur before data collection, during data analysis, or during data reporting. Censoring can be done by audits, assessment providers, or some other stakeholders.[38]

4.4 | Data transmission

It is necessary to protect data during data transmission because attacks on data and disclosure of data during data accessor transmission lead to the illegal use of patients' private information.[8]

1. Authorization and integrity: This is often guaranteed by hash functions and controlling and computing each package sent between servers and censors in the network[34,39]
2. Confidentiality: This often occurs through symmetric encryption on the traffic sent between servers and sensors. Ultimately, confidentiality is achieved by using automatically updating the key or the password.[40]
3. Availability: Access to services is provided for authorized and legal users, and reactions are shown to simultaneous access by a large number of users to services.
4. Anonymity: Patient privacy is vital in a healthcare system. Therefore, patient anonymity is guaranteed by the system. In this phase, data transmission should be done so that hackers will not be able to have access to the patients' Identifiers, identify them or restore their information.
5. Access control: While access control is performed in a partial or fine-grained manner when it comes to the data stored in servers, access control is also guaranteed in conditions where multiple individuals' writing or editing operations occur simultaneously. In such a state of access by users to data, access is prevented before necessary access policies are checked to check if the user meets the rules.[41]
6. Eavesdropping: A hacker that eavesdrops wants to have access to patients' private and sensitive medical data. Such hacking operations might occur during the communication between the patient and servers that provide healthcare or between servers that provide healthcare and cloud-based servers. For this, solutions such as forced use of access control systems should be considered to prevent conspiracy by users (patients, healthcare team, and staff) aiming at unauthorized access and receipt of medical data.[41,42]

4.5 | Data delivery

With advances in the area of cloud computing, the provision of many services or computing sources for the end user is achieved through clouds. Outsourcing data is a new paradigm in which cloud computing providers can store them as a third party. This is very cost-effective

for users because they do not need to purchase expensive hardware and software for data storage. Users are also free to manage, update, upgrade, repair, and maintain software. Private data of organizations are stored in secure and reliable sites and are provided for use from anywhere based on their requests. Confidentiality, integrity, and availability are challenging issues related to storage management and data provision.[9,43]

1. Access control: Users can access cloud-based storage servers and their private information through their specific usernames and passwords. This method can prevent unauthorized users from entering servers and stealing data. Authorized users can establish communication with cloud servers to see their private information while they cannot have access to their non-private data. This method can prevent unauthorized access by authorized users. Through a dynamic authorization mechanism, patients can sign up to receive an authorized code and access their medical data.[44,45]
2. Confidentiality: This often happens by decrypting the encrypted data at data delivery.[40] These factors were addressed in the related literature; Kelly et al.[46] mentioned confidence, privacy and security, data storage, control, and ownership as barriers to IoT-based health care. Also, other categorizations were seen in the literature: Malhotra et al.[47] categorized vulnerabilities in IoT as lack of physical security, lack of network-based security, software-based vulnerabilities, insufficient privacy protection with default settings, and insufficient audit mechanism. In addition to general ethical issues in healthcare IoT systems, specific issues such as IoT in real-time security issues have been addressed by Chen et al.[48] they have mentioned injection of malicious code, network attacks, crashing the system, for example, by DoS attacks, and extracting sensitive information by side-channel attacks. Although the authors mentioned these issues in the real-time IoT system context, they could be valid in the general IoT context. Pal et al.[49] categorized IoT security issues in an architectural layer into (1) device sensing layer, (2) network management layer, (3) Service composition layer, (4) application layer, and (5) user interface layer. In these layers, the common security issues include (1) authentication, authorization, and access control, (2) unauthorized access, modification of routing paths, (3) service authentication, data confidentiality, (4) unauthorized access, privacy leakage, integrity, and (5) authentication and authorization, and data confidentiality.

5 | CONCLUSION

What is certain is the application of IoT in the future and the existence of such a network. Although the modern technology of IoT will have many achievements in healthcare systems, it will also face numerous challenges like other emerging technologies. One of these challenges is ethical issues when large amounts of patient data are collected by objects and data computing, analyzing and storing these data by cloud-based servers and transferring these data through the network. As illustrated by the present study results, the most important ethical issues of medical IoT included security, access control, and privacy. These ethical challenges should be considered by employees and managers of organizations that use this technology. In addition to the fact that health policymakers should be aware of the moral obligation to use this technology, they should establish strict standards, regulations and policies for the use of these devices in the field of health and treatment. For example, to minimize network attacks and unauthorized access to information in the IoT, solutions such as correct configuration of application server settings, holding confidentiality and privacy training courses, determining authorized access levels and using secure information platforms are suggested.

AUTHOR CONTRIBUTIONS

Somayyeh Zakerabasali: Conceptualization; data curation; formal analysis; investigation; methodology; supervision; writing – original draft; writing – review & editing. **Seyed Mohammad Ayyoubzadeh**: Data curation; investigation; writing – original draft.

ACKNOWLEDGMENTS

The present study was conducted in collaboration with Tehran University of Medical Sciences, Health Human Resources Research Center, Shiraz University of Medical Sciences, Shiraz, Iran.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

TRANSPARENCY STATEMENT

The lead author Somayyeh Zakerabasali affirms that this manuscript is an honest, accurate, and transparent account of the study being reported; that no important aspects of the study have been omitted; and that any discrepancies from the study as planned (and, if relevant, registered) have been explained.

DATA AVAILABILITY STATEMENT

The authors confirm that the data supporting the findings of this study are available within the article and/or its Supporting Information.

ORCID

Somayyeh Zakerabasali http://orcid.org/0000-0002-1399-9234
Seyed Mohammad Ayyoubzadeh http://orcid.org/0000-0001-8450-7818

REFERENCES

1. Yazdanpanah H, Hasani. M. IoT Applications, technologies and challenges. 8th International Conference on Information and Knowledge Technology, Hamedan; 2016.
2. Habib K. Ethical aspects of the Internet of things in ehealth. *Inter Rev Inform Ethics*. 2014;22:83-91.
3. Gil D, Ferrandez A, Mora-Mora H, Peral J. Internet of things: a review of surveys based on context aware intelligent services. *Sensors*. 2016;16:1069.

4. Qin Y, Sheng QZ, Falkner NJG, Dustdar S, Wang H, Vasilakos AV. When things matter: a data-centric view of the Internet of things. Databases (csDB); Networking and Internet Architecture (csNI). 2014.
5. The Internet of Things. International Telecommunication Union (ITU) Internet Reports. 2005. Accessed July 4, 2022. https://www.itu.int/pub/S-POL-IR.IT-2005
6. Bassi A, Horn G. Internet of Things in 2020: A roadmap for the future. *European Comm Inform Soc Media*. 2008;22:97-114.
7. de Saint-Exupery A. Internet of Things strategic research roadmap. 2009.
8. Laplante PA, Laplante N. The Internet of things in healthcare: potential applications and challenges. *IT Professional*. 2016;18:2-4.
9. Dimitrov DV. Medical Internet of things and big data in healthcare. *Healthc Inform Res*. 2016;22:156-163.
10. Popescul D, Georgescu M. Internet of things—Some ethical issues. *USV Ann Econom Public Adm*. 2013;13:210-216.
11. Shamseer L, Moher D, Clarke M, et al. Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015: elaboration and explanation. *BMJ*. 2015;350:7647.
12. Hu F. Security and privacy in Internet of Things (IoTs): models, algorithms, and implementations. 2016.
13. Mittelstadt B. Designing the health-related Internet of things: ethical principles and guidelines. *Information*. 2017;8:77.
14. Chang V, Wang Z, Xu Q, et al. Smart home based on Internet of Things and ethical issues. 2021. doi:10.5220/0010178100570064
15. El-Khoury M, Arikan C. From the Internet of things toward the Internet of bodies: ethical and legal considerations. *Strateg Change*. 2021;30:307-314.
16. Baldini G, Botterman M, Neisse R, Tallacchini M. Ethical design in the Internet of things. *Sci Eng Ethics*. 2018;24:905-925.
17. Karale A. The challenges of IoT addressing security, ethics, privacy, and laws. *Internet Things*. 2021;15:100420.
18. Philip N, Rodrigues J, Wang H, Fong S, Chen J. Internet of things for in-home health monitoring systems: current advances, challenges and future directions. *IEEE J Sel Areas Commun*. 2021;39:300-310.
19. Aledhari M, Razzak R, Qolomany B, Al-Fuqaha A, Saeed F. Biomedical IoT: enabling technologies, architectural elements, challenges, and future directions. *IEEE Access*. 2022;10:31306-31339.
20. Olawole A. Security and privacy consideration for Internet of things in smart home environments. 2022.
21. Nadian-Ghomsheh A, Farahani B, Kavian M. A hierarchical privacy-preserving IoT architecture for vision-based hand rehabilitation assessment. *Multimed Tools Appl*. 2021;80:1-24.
22. Lhotska L, Cheshire P, Pharow P, Macku D. Non-technical issues in design and development of personal portable devices. *Stud Health Technol Inform*. 2016;221:46-50.
23. Furstenau LB, Rodrigues YPR, Sott MK, et al. Internet of things: conceptual network structure, main challenges and future directions. *Digit Commun Netw*. Published online May 2, 2022. doi:10.1016/j.dcan.2022.04.027
24. Somayyeh N, Akhavan. P. Ethics in information technology: challenges and roots. The first regional conference on new approaches in computer engineering 2011; Roudsar.
25. Barchard KA. Ethics in online data collection. Presentation at: the Western Psychological Association Annual Convention. May 2, 2013. Vancouver, BC.
26. UNICEF. *Procedure for Ethical Standards in Research, Evaluation, Data Collection and Analysis*; 2015.
27. Ahmad Ghaderi FM. Principles of informed consent in medicine. *Koomesh*. 2014;15:133-137 (in persian).
28. Mohammadzadeh N, Safdari R, Rahimi A. Multi-agent system as a new approach to effective chronic heart failure management: key considerations. *Healthc Inform Res*. 2013;19:162-166.
29. Brewster P. The ethics and security of cloud computing. 2013. Accessed July 4, 2022. https://www.legalsupportnetwork.co.uk/practice-management/resources/ethics-and-security-cloud-computing
30. Ziegeldorf J, Garcia Morchon O, Wehrle K. Privacy in the Internet of things: threats and challenges. *Secur Commun Netw*. 2014;7:2728-2742.
31. Mittelstadt B. Ethics of the health-related Internet of things: a narrative review. *Ethics Inf Technol*. 2017;19:157-175.
32. Sun Y, Zhang J, Xiong Y, Zhu G. Data security and privacy in cloud computing. *Int J Distrib Sens Netw*. 2014;10.
33. Chen D, Zhao H. Data security and privacy protection issues in cloud computing. Paper presented at: International Conference on Computer Science and Electronics Engineering, Hangzhou, Zhejiang, China, March 23-25, 2012.
34. Boonyarattaphan A, Yan B, Sam C. A security framework for e-Health service authentication and e-Health data transmission. Paper presented at: 2009 9th International Symposium on Communications and Information Technology, Incheon, Korea (South), September 28-30, 2009.
35. Aldossary S, Allen W. Data security, privacy, availability and integrity in cloud computing: issues and current solutions. *Inter J Advan Computer Sci Appl*. 2016;7. doi:10.14569/IJACSA.2016.070464
36. Leviathan Security Group. Comparison of availability between local and cloud storage. 2015. Accessed November 18, 2017. https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad9ae4b069728afca34a/1436396954508/Value%2Bof%2BCloud%2BSecurity%2B-%2BAvailability.pdf
37. Patel AA, Nirmala SJ, Bhanu SMS. *Security and Availability of Data in the Cloud*. Springer Berlin Heidelberg; 2012:255-261.
38. Mark MM, Eyssell KM, Campbell B. The ethics of data collection and analysis. *New Dir Eval*. 1999;1999:47-56.
39. Shahzad M, Singh MP. Continuous authentication and authorization for the Internet of things. *IEEE Internet Comput*. 2017;21:86-90.
40. Nath S, Som S. Security and privacy challenges: Internet of things. *Indian J Sci Technol*. 2017;10.
41. Othman SB, Bahattab AA, Trad A, Youssef H. Secure data transmission protocol for medical wireless sensor networks. Paper presented at: 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, Victoria, BC, Canada, May 13-16, 2014.
42. Dyer KA. Ethical challenges of medicine and health on the Internet: a review. *J Med Internet Res*. 2001;3:E23.
43. Mohammadzadeh N, Safdari R, Rahimi A. Cancer care management through a mobile phone health approach: key considerations. *Asian Pac J Cancer Prev*. 2013;14:4961-4964.
44. Wang X, Chen F, Ye H, et al. Data transmission and access protection of community medical Internet of things. *J Sens*. 2017;2017:14.
45. Popescul D, Bayer Y. Ethical concerns and solutions in Health Internet of Things. 2018.
46. Kelly J, Campbell K, Gong E, Scuffham P. The Internet of things: impact and implications for healthcare delivery. *J Med Internet Res*. 2020;22 (preprint). doi:10.2196/20135
47. Malhotra P, Singh Y, Anand P, Bangotra DK, Singh PK, Hong WC. Internet of things: evolution, concerns and security challenges. *Sensors*. 2021;21:1809.
48. Chen CY, Hasan M, Mohan S. Securing real-time Internet-of-Things. *Sensors*. 2018;18.
49. Pal S, Hitchens M, Rabehaja T, Mukhopadhyay S. Security requirements for the Internet of things: a systematic approach. *Sensors*. 2020;20:5897.

How to cite this article: Zakerabasali S, Ayyoubzadeh SM. Internet of Things and healthcare system: a systematic review of ethical issues. *Health Sci Rep*. 2022;5:e863. doi:10.1002/hsr2.863