Original Article

Health, Spirituality and Medical Ethics. 2020;7(4):25-32

Identifying and Ranking Ethical Issues of the Internet of Things in Medical Sciences using Stepwise Weight Assessment Ratio Analysis

Received 22 Feb 2020; Accepted 24 Oct 2020
http://dx.doi.org/10.29252/jhsme.7.4.25

Mohammad Hossein Ronaghi[1*], Hanieh Mohammadi[1]

1 Department of Management, College of Economics, Management and Social Sciences, Shiraz University, Shiraz, Iran.

Abstract

Background and Objectives: The Internet of Things (IoT) refers to billions of physical devices around the world that are now connected to the internet, all collecting and sharing data. The IoT has been widely applied to interconnect available medical resources and provide reliable, effective and smart healthcare service to the people. The social acceptance of IoT applications and services strongly deepens on the trustworthiness of information and the protection of private data. The marked expansion of the IoT specific technologies has presented daunting ethical challenges. Therefore, the present study aimed to identify the ethical issues of IoT in medical sciences in Iran.

Methods: The current study was conducted in two phases using the mixed-method approach in winter 2020. In the first phase, the ethical issues of the IoT were identified by library search and assessed by the content analysis. In the second phase, ethical issues were ranked by a panel of experts, including 15 IT experts who worked in medical universities in Iran. The Stepwise Weight Assessment Ratio Analysis (SWARA) method was used for ranking the ethical issues of IoT.

Results: The obtained results revealed the importance of informed consent (0.259), privacy (0.227), information security (0.195), trust (0.171), and physical safety (0.148) in ethical issues of IoT.

Conclusion: As evidenced by the obtained results, informed consent and privacy were the most important ethical issues in IoT. Moreover, IoT devices that target or profile peoples' information without their knowledge or consent could be interpreted as infringing upon their privacy. The users of these devices should be able to intentionally manage the transformative effects of the technologies that influence and shape their development. Moreover, the health sector policymakers should be aware of the ethical commitment to using IoT technology.

Keywords: Ethics, Internet of Things, Medical Sciences.

***Correspondence:** Should be addressed to Dr. Mohammad Hossein Ronaghi. **Email:** mh_ronaghi@shirazu.ac.ir

Please Cite This Article As: Ronaghi MH, Mohammadi H. Identifying and Ranking Ethical Issues of the Internet of Things in Medical Sciences using Stepwise Weight Assessment Ratio Analysis. Health Spiritual Med Ethics. 2020;7(4):25-32.

Introduction

The use of the Internet as a global communication network has undergone a dramatic change which enables millions of machines and smart objects to connect and cooperate with each other. This technology is known as the Internet of Things (IoT) (1) which exchanges information through a variety of devices and tools with different connections. These objects work together to create new applications, provide services, and achieve common goals. The IoT aims to enable objects to connect to every device or person that can receive or send information via any path or network at any time and place (2).

Due to the growing trend of IoT, it is predicted that by the end of 2020, about 50 billion objects will have been connected to the Internet (3). This connectivity has attracted the attention of companies,

governments, and citizens around the world and has resulted in a parallel increase in research in industry and universities (4). Within the domain of IoT, each object can be uniquely defined and equipped with sensors in the form of an Internet network. Today, the Internet and its related tools are dramatically integrated into the lives of individuals and businesses (5).

IoT technology uses IP-based Service-Oriented Architecture (SOA) to create integration and interaction among the components (6). The IoT is used in various industries, including a technology that has revolutionized medical care and is used to monitor people and collect patient information. It is projected that about 40% of IoT technology services will be related to the healthcare domain by the end of 2020 (7). The need for telecommunications equipment and their effective use has been proved in the field of healthcare and medicine due to such factors as massive amounts of medical data, time strains in data analysis, the importance of transaction speed, as well as high sensitivity and accuracy.

The IoT can be used in a variety of medical fields, including remote patient care systems, emergency alert systems, fitness programs, chronic illnesses, and geriatric care. These applications may include heart rate monitoring systems, blood pressure measuring systems, health monitoring systems, artificial pacemakers, wearable sensors, and hearing aids (8, 9). The users' unawareness and the development of this technology have led to various vulnerabilities and attacks on IoT systems. These vulnerabilities have been exacerbated by the widespread use of new technologies, such as Radio Frequency Identification (RFID), Near Field Communication (NFC), sensors, as well as the third, fourth, and fifth generation telecommunications networks, leading to the emergence of Information security threats and new risks in this new environment (10).

The IoT uses sensors and trackers to identify and track different devices and people. Despite the unlimited benefits of this technology, it poses numerous challenges, especially to the security and privacy of individuals. It is of utmost importance to address these issues and observe ethical considerations. The users need to trust the security of IoT devices and their related services; moreover, it is vital to consider social behaviors, the ethical use of technologies, and the safety of these systems (11). The regulation of social relations based on ethical principles assumes critical importance in the use of various technologies. In numerous work and life domains, if people do not adhere to moral principles, there is no detrimental external force to deter them from violating each other's rights (12).

Informed consent is the mainstay of ethics and law, and stakeholders reserve the right to obtain information and ask questions (13). Informed consent in medical ethics has received assiduous attention and consideration, especially in the last few decades. Nonetheless, this concept dates back to ancient medicine and was fundamentally developed in the 19th and 20th centuries (14). The concept of informed consent is explained in citizens' interaction with the digital to regulate behavior with personal data since the consent of a data source (e.g., a patient or citizen) is often necessary for the user to process and legitimately use personal data.

To provide informed consent for the application of personal data, the users must have a sound knowledge of how their personal information will be used by the applications and equipment. People with inadequate information and expertise in the information and communication technology may find it difficult to develop such awareness (15). Accordingly, based on the ethical principles, every technology must be used with the full knowledge of the user. In this regard, transparent information regarding the use of personal information should be provided in the form of an agreement.

Many IoT devices and tools may have low-level and inefficient information security (16, 17). IoT security is one of the daunting challenges presented to the successful implementation of IoT devices. The ease of connecting and accessing IoT devices has increased the possibility of serious security issues. Moreover, this trend is on the rise due to the widespread distribution of heterogeneous

devices and their possible connection without requesting a license or even informing their owners (11).

Uncontrolled environment, heterogeneity, scalability, and resource restraints are recognized as the main features of the IoT (1). Therefore, the data collected by various cameras and microphones may be sent by smart displays and other similar devices to the manufacturer's servers for data analysis without the knowledge and consent of users (18). Technical analysis is a major part of the security issues in IoT devices, that is to say, although many components have some security features, such as passwords to restrict user access, these passwords are typically set to factory defaults and never change (19).

In addition, default passwords are available online (20); consequently, experts can hack these devices intentionally or out of curiosity, thereby violating privacy and affecting security issues (21). In terms of information security, any device or portal should have a 32-character password that requires uppercase and lowercase letters, numbers, and symbols; moreover, this password should be changed on a daily basis. Nevertheless, this is only the technical aspect of security issues, and specialized training on the use of devices is necessary to achieve higher security (4).

There is controversy over the issues of IoT privacy and security since IoT devices can analyze and share large amounts of user data (22). Even in the event of public awareness of privacy breaches on the Internet, in IoT development, these risks are likely to increase due to the massive amount of collected and processed data. This data may be related to individuals and patients, their daily activities, the increasing relationship between the digital world and real life, and the use of new devices and tools, such as wearable sensors in the medical field (23).

Some measures are being implemented to protect the privacy of cyberspace users; however, the majority of legal challenges of IoT have not been addressed yet. The General Data Protection Regulation (EU GDPR) has been involved in this field for several years and has initiated fundamental measures to increase data protection. Courts also set an agenda for the recognition of digital privacy rights (4). Finally, the IoT, with its numerous sensors and integrated communications, provides a good opportunity to gather personal information which can significantly affect a person's privacy.

Therefore, the privacy of people using the IoT can be protected by the following measures: setting strict rules to protect the confidentiality of user data, assigning specialized judicial units for possible problems in this area, and informing people about how their personal information would be used. One of the differences between IoT and the traditional Internet is the active nature of the equipment and objects in the real world and the surrounding environment. One of the ethical priorities is to reduce or eliminate the disadvantages of using these tools and equipment (24).

One of the effective measures to prevent physical damage or undesirable threats is the hardware safety of the IoT which protects the environment from such damages. In this regard, it is indispensable to develop an IoT system with high security and reliability to create newly designed architectures that provide a safe and secure system environment (11). Physical safety in the IoT means planning and rational prediction of the behavior of equipment, as well as preventing unexpected and unwanted behaviors (25). One of the main pillars of the physical safety of devices is the supervision of government and executive bodies, as well as the establishment of safety standards. This is also reflected in the design of vehicles and production equipment in the field of IoT (26).

Trust in the IoT means that the behavior of users and technology developers would be predictable if system components do their job properly (27). Trust in IoT is a matter of great concern which can be aggravated by the interaction among objects. Three categories of IoT trust must be addressed: trust in a “thing,” (2) trust in a network of “things,” and (3) trust that the environment and context that the network will operate in is known and that the network will be fit for purpose in that

environment, context, and at a specific point in time (28). Considering the mutual interaction between trust and ethics (29), it can be concluded that gaining the trust of users in the field of IoT is a moral behavior which increases the trust of the audience.

Due to the importance of IoT technology in the field of medicine, in their study, Ronaghi and Hosseini ranked IoT services in the field of health using the fuzzy analytic hierarchy process. The results of the mentioned study showed that the management of chronic diseases and emergency medical services are given priority. It was also found that policymakers in the field of IoT technology should first be aware of the role of this technology in saving lives. As the next priority, investment in IoT can help control and monitor the behaviors of the elderly, patients, and children (30).

In another study, the existing literature on effective ways of designing the IoT in the field of medical care was first critically evaluated. Thereafter, a new semantic model is proposed for patients' electronic health using four layers of sensors, network layer, internet layer, and service layer (31). Along the same lines, Mahbanooei et al. identified and ranked the E-Health Codes of Medical Ethics. In the referred research, the snowball method was used for sampling and the fuzzy hierarchical analysis method was used for data analysis. The results of this study demonstrated that among the E-Health codes of medical ethics, privacy, increasing the quality of e-services, and professionalism in online health care take on an added importance in hospitals (32).

In their study, Atlam and Wills examined the security and confidentiality of the IoT and analyzed the security of smart cities from different perspectives (11). Compared to previous studies, there is a research gap regarding the importance of the challenges presented by the use and localization of the IoT in Iran. In light of the aforementioned issues, the present study aimed to identify and rank the ethical challenges presented by IoT technology in the field of medical sciences from the perspective of Iranian experts.

Methods

The applied research was conducted using the combined method in the winter of 2019. In the first part of the research, the related studies and articles in the field of IoT ethics were reviewed, and the relevant codes were extracted using the content analysis method. In the second part, Stepwise Weight Assessment Ratio Analysis (SWARA) method was used to rank moral indicators. It is one of the multi-criteria decision-making methods that was developed by Kersuliene et al. in 2010 which enables decision-makers to select, evaluate, and weigh the indicators (33).

The greatest advantage of this method over similar methods lies in its ability to evaluate the accuracy of experts' opinions about the weighted indicators during the method process. In addition, experts can consult with each other which makes the results more accurate, compared to other multi-criteria decision-making methods (34). The main steps of weighting based on the SWARA method are as follows (33):

Step 1: Sorting the indicators

Step 2: Determining the relative importance of each indicator (Sj)

Step 3: Calculating the coefficient Kj. The Kj coefficient which is a function of the relative importance of each indicator is calculated using Equation 1.

$$K_j = S_j + 1 \qquad \text{Equation 1}$$

Step 4: Calculating the initial weight of each indicator: the initial weight of the indicators can be calculated using Equation 2. In this regard, it should be noted that the weight of the first indicator, which is the most important indicator, is considered equal to 1.

$$q_j = \frac{q_{j-1}}{K_j} \qquad \text{Equation 2}$$

Step 5: Calculating the final normal weight: in the last step of the SWARA method, the final weight of the indicators, which is also considered the normalized weight, is calculated by Equation 3.

$$W_j = \frac{q_j}{\sum q_j} \qquad \text{Equation 3}$$

The panel of research experts included 15 managers and information technology experts working in medical universities. They were selected due to their familiarity with IoT technology, as well as 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.

Result

Based on the results of library studies, five factors were identified as ethical challenges in the field of IoT. The results of the content analysis are displayed in Table 1.

Table 2 illustrates the results of weighting based on the SWARA method. The informed consent (0.259) and privacy (0.227) were given the most weight, followed by information security (0.195), trust (0.171), and physical safety (0.148), respectively.

Table 1. Ethical challenges in the field of the internet of things

Ethical issue	Sources
Informed consent	(13), (14), (15)
Information security	(4), (11), (16), (17), (18), (19), (20), (21)
Physical safety	(4), (24), (25), (26), (27)
Privacy	(4), (11), (22), (23)
Trust	(28), (29)

Table 2. Results of the weighting of ethical indicators using the SWARA method

Indicators	Relative importance	Kj	Initial weight qj	Standard weight Wj
Informed consent	-	1	1	0.259
Privacy	0.149	1.141	0.875	0.227
Information security	0.158	1.158	0.756	0.195
Trust	0.141	1.141	9.662	0.171
Physical safety	0.166	1.166	0.576	0.148

Discussion

IoT technology has risen in importance due to the increasing growth of smart tools, network communication, various tools, and equipment. The IoT has a wide application in different fields, including medical science and health; nonetheless, it is presented with numerous challenges as other innovative technologies do. In this regard, the way of data transmission among the devices has given rise to daunting ethical challenges in this field. Therefore, the present study sought to identify and rank the ethical challenges presented to the IoT in medical sciences. Based on the results, users' awareness and informed consent were the most important ethical challenge in this field from the perspective of medical experts.

In the same vein, in a study performed by Allhoff and Henschke (4), informed consent was introduced as one of the ethical issues in the field of IoT technology. Due to the possibility of access to personal information of patients and users of smart tools, people must be aware of the amount and type of the exchanged information; therefore, in the first instance, the user should acknowledge this possibility. Privacy was the second most important indicator from the experts' point of view. The studies conducted by Weber (22) and Baldini et al (23) also highlighted the importance of privacy in the use of the IoT.

In this regard, to observe privacy, people must have controlled access to network data. The next priority of ethical challenges was information security. This finding is consistent with the results of the studies carried out by Atlam and Wills (11), Urquhart and McAuley (17), and Ronaghi and Hosseini (30). Accordingly, the method of information transmission in the network and prevention of network attacks help to manage network security. Trust has become one of the challenges faced by the users of this technology due to the newness of IoT technology, some users' insufficient knowledge, as well as the remote controls of various network devices. Accordingly, building trust in users and patients using IoT equipment and awareness-raising in this area can facilitate the implementation of IoT technology. Physical safety was identified as the last ethical challenge in the field of IoT. This security can be enhanced by the use of well-known

equipment and sensor manufacturers, the conclusion of contracts with experienced companies in the field of IoT, and network controls.

One of the limitations of the present study was the evaluation of ethical challenges from the perspective of experts. Therefore, it is suggested that the views of patients and users of IoT tools be assessed in future research. Furthermore, is recommended that indeterminate techniques, such as fuzzy and grey methods, be applied to obtain real information in the evaluation of people's opinions.

Conclusion

IoT technology has wide applications in medicine, such as fall detection, wearable sensors, and remote continuous monitoring of patients. As illustrated by the results of the present study, the most important ethical challenges of medical IoT included informed consent and privacy. Therefore, health policymakers should issue stringent regulations on the application of these devices in the field of healthcare and medicine. These regulations should be developed based on information dissemination and obtaining the consent of patients and users so that executives will be required to inform patients about these issues. As a final note, to minimize network attacks and unauthorized access to information and maintain information security in IoT, it is suggested to properly configure the application server settings, run training courses on information confidentiality, and use secure information platforms, such as firewalls.

Conflict of interest

The authors declare that they have no conflict of interest regarding the publication of the present article.

Acknowledgements

The authors' deepest appreciation goes to all experts for their collaboration in data collection.

References

1.Janbabaei S, Gharaee H, Mohammadzadeh N. The lightweight authentication scheme with capabilities of anonymity and trust in internet of things (IoT). Signal Data Proc 2019;15(4):111-22. (In Persian) Link
2.Ronaghi MH, Forouharfar A. A contextualized study of the usage of the Internet of things (IoTs) in smart farming in a typical Middle Eastern country within the context of Unified Theory of Acceptance and Use of Technology model (UTAUT). Technol Soc 2020;63:101415. Link
3.Mekala MS, Viswanathan P. CLAY-MIST: IoT-cloud enabled CMM index for smart agriculture monitoring system. Measurement 2019;134:236-44. Link
4.Allhoff F, Henschke A. The internet of things: Foundational ethical issues. Internet Things 2018;1:55-66. Link
5.Castaneda C. Internet of things to become cornerstone of excellent customer service. India: Finds Frost & Sullivan; 2015. Link
6.Khanna A, Kaur S. Evolution of Internet of Things (IoT) and its significant impact in the field of Precision Agriculture. Comput Electron Agr 2019;157:218-31. Link
7.Tavakoli M, Razeghi H, Nasiripoor A. The effect of using internet of things on organizational performance in health-related issues (Case study: Shahid Rajaee hospital in Tehran). J Healthcare Manag 2017;8(2):43-66. (In Persian) Link
8.Salunke P, Nerkar R. IoT driven healthcare system for remote monitoring of patients. J Modern Trend Sci Technol 2017;3(6):100-3. Link
9.Baker S, Xiang W, Atkinson I. Internet of things for smart healthcare: technologies, challenges and opportunities. IEEE Access 2017;5:26521-44. Link
10.Popescul D, Georgescu M. Internet of things–some ethical issues. USV Ann Econ Public Administ 2014;13(2):208-14. Link
11.Atlam HF, Wills GB. IoT security, privacy, safety and ethics. Digital Twin Technologies and Smart Cities. Berlin, Germany: Springer; 2020. Link
12.Khanifar H, Bazaz Z, Molavi Z. Philosophy of ethics in management science. Sci J Islamic Manag 2020;23(1):137-58. (In Persian) Link
13.American Medical Association. American medical association's code of medical ethics. New York: Opinion E-8.056; 2016. Link
14.Katz J. Informed consent-must it remain a fairy tale. J Contemp Health L Pol'y 1994;10:69. Link
15.Neisse R, Baldini G, Steri G, Miyaki Y, Kiyamoto S, Biswas A. An agent-based frame-work for informed consent in the internet of things. Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy; 2015. P. 789-94. Link
16.Chapman E, Uren T. The internet of insecure things. Canberra: Australian Strategic Policy Institute; 2018. Link
17.Urquhart L, McAuley D. Avoiding the internet of insecure industrial things. Comput Law Security Rev 2018;34(3):450-66. Link
18.Chokshi N. Is Alexa listening? Amazon echo sent out recording of couple's conversation. New York: New York Times; 2018. Link
19.Kan M. IoT botnet highlights the dangers of default passwords. San Francisco: InfoWorld; 2016. Link
20.Hiner J. New research: most Iot devices can be hacked into botnets. California: TechRepublic; 2018. Link
21.Kobie N. The internet of things: convenience at a price. London: The Guardian; 2015. Link
22.Weber RH. Internet of things: privacy issues revisited. Comput Law Security Rev 2015;31(5):618-27. Link
23.Baldini G, Botterman M, Neisse R, Tallacchini M. Ethical design in the internet of things. Sci Eng Ethics 2018;24(3):905-25. Link
24.Lin P, Abney K, Bekey GA. Robot ethics: the ethical and social implications of robotics. Intelligent robotics and

autonomous agents' series. Massachusetts: MIT Press; 2012. Link
25.Agarwal Y, Dey A. Toward building a safe, secure, and easy-to-use internet of things infrastructure. IEEE Comput 2016;49(4):88-91. Link
26.Mak S, Lau H. An enhanced safety assessment model for toy products. Proceedings of the IEEE Symposium on Product Compliance Engineering, Austin, TX, USA; 2014. P. 24-8. Link
27.Uslaner EM. The moral foundations of trust. Cambridge: Cambridge University Press; 2010. Link
28.Voas, J, Kuhn R, Laplante P, Applebaum S. Internet of things (IoT) trust concerns (draft). Maryland: National Institute of Standards And Technology; 2018. Link
29.Mehrgan F, Sobhi E. Analysis of the structural relationship between the organizational trust with the self-efficiency and professional ethics among nurses. Quart J Nurs Manag 2020;8(4):41-51. (In Persian) Link
30.Ronaghi M, Hosseini F. Identifying and ranking IoT services in healthcare sector. J Health Administ 2018; 21(73):29-41. (In Persian) Link
31.Ullah K, Shah MA, Zhang S. Effective ways to use internet of things in the field of medical and smart health care. International Conference on Intelligent Systems Engineering (ICISE), Islamabad, Pakistan; 2016. P. 372-9. Link
32.Mahbanooei B, Poorezat A. Identifying and ranking e-health cods of medical ethics. Ethics Sci Technol 2019; 14(3):29-36. (In Persian) Link
33.Keršulienė V, Zavadskas E, Turskis Z. Selection of rational dispute resolution method by applying new step-wise weight assessment ratio analysis (SWARA). J Busin Econ Manag 2010;11(2):243-58. Link
34.Heidari J, Mohamadi N, SalarVanaki A, Ghafari S. A hybrid approach for selecting appropriate technological forecasting technique. J Technol Dev Manag 2017;4(4):163-94. (In Persian) Link

شناسایی و رتبه‌بندی مسائل اخلاقی اینترنت اشیا در علوم پزشکی با استفاده از روش سوارا

تاریخ ارسال: ۱۳۹۸/۱۲/۰۳؛ تاریخ پذیرش: ۱۳۹۹/۰۸/۰۳

محمدحسین رونقی[۱*]، حانیه محمدی[۱]

[۱] بخش مدیریت، دانشکده اقتصاد، مدیریت و علوم اجتماعی، دانشگاه شیراز، شیراز، ایران.

چکیده

سابقه و هدف: اینترنت اشیا به جمع‌آوری و تسهیم داده‌های میلیاردها وسایلی که از طریق اینترنت در سراسر دنیا به یکدیگر متصل شده‌اند، اشاره دارد. اینترنت اشیا به طور گسترده‌ای برای اتصال منابع پزشکی موجود و ارائه خدمات مطمئن، مؤثر و هوشمند سلامت به افراد استفاده می‌شود. پذیرش کاربردها و خدمات اینترنت اشیا به محافظت از داده‌های خصوصی و اعتماد به اطلاعات وابسته می‌باشد. گسترش چشمگیر فناوری‌های خاص اینترنت اشیا، چالش‌های اخلاقی مهمی را به همراه داشته است. در این راستا، مطالعه حاضر با هدف شناسایی مباحث اخلاقی اینترنت اشیا در علوم پزشکی ایران انجام شد.

روش کار: پژوهش حاضر در دو مرحله با استفاده از روش ترکیبی در زمستان ۱۳۹۸ انجام شد. در مرحله اول، مسائل اخلاقی اینترنت اشیا با جستجوی کتابخانه‌ای و روش تحلیل محتوا شناسایی شدند. در مرحله دوم نیز مسائل اخلاقی توسط گروهی از خبرگان شامل ۱۵ نفر از متخصصان فناوری اطلاعات که در دانشگاه‌های علوم پزشکی ایران فعالیت می‌کردند، رتبه‌بندی گردیدند. از روش سوارا برای رتبه‌بندی مسائل اخلاقی اینترنت اشیا استفاده شد.

یافته‌ها: یافته‌های به دست آمده حاکی از آن هستند که رضایت آگاهانه (۰/۲۵۹)، حریم خصوصی (۰/۲۲۷)، امنیت اطلاعات (۰/۱۹۵)، اعتماد (۰/۱۷۱) و ایمنی فیزیکی (۰/۱۴۸) دارای بیشترین اهمیت در بین مسائل اخلاقی اینترنت اشیا می‌باشند.

نتیجه‌گیری: با توجه به نتایج به دست آمده می‌توان گفت که رضایت آگاهانه و حفظ حریم خصوصی، مهم‌ترین مسائل اخلاقی در اینترنت اشیا هستند. دستگاه‌های اینترنت اشیا که بدون اطلاع و رضایت کاربران، اطلاعات افراد را استفاده می‌کنند، ممکن است به عنوان ناقض حریم خصوصی تلقی شوند. کاربران این دستگاه‌ها باید بتواند به طور آگاهانه از اثرات این فناوری‌ها و روند توسعه آن‌ها مطلع باشند. علاوه‌براین، سیاست‌گذاران بخش سلامت باید از تعهد اخلاقی نسبت به استفاده از فناوری اینترنت اشیا آگاه باشند.

واژگان کلیدی: اخلاق، اینترنت اشیا، علوم پزشکی.

* **نویسنده مسئول:** محمدحسین رونقی. ایمیل: mh_ronaghi@shirazu.ac.ir