Letter to Editor Open Access

Standardization challenges in the IOT and AI era

M. M. Share Pasand[1*]
1. Electrical Engineering Research Group, Research Center of Technology and Engineering, Standard Research Institute, Karaj, Iran

Dear Editor

The Internet of Things (IOT) and Artificial Intelligence (AI) are being increasingly utilized in industrial, household and business sectors expected to change many aspects of the human life. As the nearly infinite possibilities unveil, many people even the expert ones, feel threatened [1, 2]. Calls to manage the risks or restrict the growth of these new trends, make us think about how severely the implications of this growth may change our lives. Human is being surrounded by AI enabled devices which are capable of communicating to each other through IOT. This combination sounds even more threatening than AI or IOT alone. In fact, we are at the edge of believing to be manipulated rather than making use of these newly emerging technologies. What role a standardization body can accomplish in this situation?

1 Emerging concerns

Standards have been widely used to ensure that specific goals (including user safety, environmental compatibility, sustainable development [3], etc.) are fulfilled for a product or service. With IOT and AI appearing in almost any technological product, we have new concerns. Some of the most important of these concerns are listed below [4-6].

1-1 Human intervention

If a process is done by a computer via AI or any automated algorithm, there should always be levers to facilitate human intervention in the process. The AI should not be able to disable or skip human intervention. This is to ensure that ethics and regulations are not violated.

1-2 Privacy

The development of AI and IOT technologies should consider privacy. AI may be capable to use acquired data to infer something personal about people.

This private information may be consequently communicated to other entities through IOT. The receiving entity may have different governing rules and possibilities. Other people may become aware and make illegal or immoral use that information. Standards should set limits and regulations regarding privacy.

1-3 Transparency

Any decision, modification or analysis performed within the AI machine should be transparent and visible to the user and operator. Similarly, any communication performed via IOT should be traceable and transparent. AI and IOT assisted technologies should be equipped by data logs to record whatever happens both from the outside or inside of the machine.

1-4 Impartiality

AI and IOT based technologies should not impose or cause any discrimination based on gender, race, ethnicity, etc. This becomes more important when AI tries to classify people according to automatically extracted features and characteristics.

No advantage/ disadvantage may be caused during any of these classifications and the consequent decisions should be impartial. Impartiality should also be considered in data processing and recording. AI should not be allowed to use/ record information in unjust ways.

* Correspondence:
sharepasand@standard.ac.ir

1-5 Legal responsibility
For any action by an AI technology the manufacturer/ operator company should be held legally responsible. If the data contributing to any decision/ action with legal consequences was communicated to AI, via an IOT enabled technology, then the IOT provider should bear its share of responsibility. This should be reflected in law as well as the standards.

1-6 Restricted actions
Proportionate to its capabilities, each AI assisted technology should have a list of restricted action which cannot be altered or removed. These include causing harm to living beings, illegal activities, etc. The items on such a list are ultimately dependent to how that specific AI categorizes and classifies actions.

2 Conclusion and discussion
The aforementioned concerns should be systematically incorporated into the standardization process. This implies that any of the four major facets of standardization namely; metrology, standard development, conformity assessment and accreditation may be affected. In the following, the implications of these emerging concerns are discussed.

2-1 Metrology
It is important to develop consensus based quantifiable metrics to the aforementioned concerns and to measure for instance, privacy, discrimination, etc.
Risk assessment [7] may also be required to quantify the risk of any suspicious activity. The uncertainty of the assigned values should be determined.

2-2 Standard development
Technical experts developing standards should be aware of these concerns and should find effective ways to practically and rigorously incorporate them in the standards.

2-3 Conformity assessment
A certification body should have sufficient tools and professional personnel to determine whether an AI/ IOT assisted product/ system conforms to the standards requiring privacy, impartiality, etc.

2-4 Accreditation
Accreditation bodies should be able to examine the capability and competency of a conformity assessment body in evaluating the emerging concerns in an AI/ IOT assisted product/ system.

Funding
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declarations
Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Received: Mar. 2023 Accepted: Apr. 2023
Published online: Apr. 2023

DOI: 10.22034/ASAS.2023.403442.1023

References
[1] https://www.nbcnews.com/politics/joe-biden/biden-meets-ai-experts-effort-manage-risks- rcna90136
[2] Taddeo, Mariarosaria, Tom McCutcheon, and Luciano Floridi. "Trusting artificial intelligence in cybersecurity is a double-edged sword." Nature Machine Intelligence 1.12 (2019): 557-560.
[3] https://www.iso.org/sdgs.html
[4] IEC white paper: safety in future: 2020.
[5] European Commission, White Paper on Artificial Intelligence – A European approach to excellence and trust. 2020.
[6] Manziuk, Eduard, et al. "Formal Model of Trustworthy Artificial Intelligence Based on Standardization." IntelITSIS. 2021.
[7] ISO 31000. Risk Management. International standardization organization. 2018.