4th International Conference on
Combinatorics, Cryptography, Computer Science and Computing
November 20-21, 2019 - Iran University of Science & Technology

Standardization for the Internet of Things

Hamidreza Damghani [1], Heliasadat Hosseinian [2], Leila Damghani [3] Faramarz Faghihi [4]

[1] Faculty of Mechanics, Electrical and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran.

hamidreza.damghani@gmail.com

[2] Faculty of Mechanics, Electrical and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran.

helia.hosseinian@aut.ac.ir

[3] Faculty of Computer Engineering- Artificial intelligence, Kharazmi University, Tehran, Iran.

Damghani.iau@gmail.com

[4] Faculty of Mechanics, Electrical and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran.

Faramarz.faghihi@srbiau.ac.ir

ABSTRACT

The Internet of Things (IoT) alludes to gadgets that are frequently obliged in correspondence and calculation abilities, presently ending up more regularly associated with the Internet, and to different administrations that are based over the capacities these gadgets together give. It is normal that this improvement will introduce more machine-to-machine (M2M) correspondence utilizing the Internet with no human client effectively included. Specialized principles empower the handling of information and take into consideration the interoperability of accumulated informational indexes. Soon, we could see orders from industry consortia or potentially measures bodies identified with specialized and administrative IoT gauges. This paper reviews a few guidelines by IEEE, ISO, IEC, IETF, and ITU that empower innovations empowering the fast development of IoT. These principles incorporate correspondences, directing, system and session layer conventions that are being created to meet IoT necessities.

KEYWORDS: Internet of Things; IoT standards; IoT protocols; IoT security; Standardization.

1 INTRODUCTION

1-1 Overview

Accumulation is accomplished using different gauges relying upon the IoT application nearby. As indicated by the International Organization for Standardization (ISO), "a standard is an archive that gives necessities, details, rules or qualities that can be utilized reliably to guarantee that materials, items, procedures, and administrations are fit for their motivation [1].

- Choice and notice: The standard of decision and notice expresses that elements that gather information should give clients the choice to pick what they uncover and advise clients when their own data is being recorded. This may not be required for IoT applications that total data, delinked to a particular person.

- Purpose determination and use constraint: This rule expresses that substances gathering information should obviously express the reason for the expert that allows the accumulation of that information. The utilization of information must be constrained to the reason determined, in spite of the fact that this may obstruct imaginative employment of gathered informational indexes in different IoT applications.

- Data minimization: The guideline of information minimization recommends that an organization can gather just the information required for a particular reason and erase that information after the planned use. This essentially confines the extent of investigation that can come about because of cutting and dicing the IoT information.

- Security and responsibility: This guideline expresses that elements that gather and store the information are responsible and must send security frameworks to maintain a strategic distance from any unapproved get to change, erasure, or utilization of the information.

We just examined the issues identified with administrative measures. Innovation norms, the second kind, involves three components: organize conventions, correspondence conventions, and information conglomeration measures [2].

- Network conventions: Network conventions allude to a lot of principles by which machines recognize and approve one another. Interoperability issues result from numerous system conventions in presence. As of late, organizations in the IoT esteem chain have started cooperating to help adjust numerous system conventions. One precedent is the AllJoyn standard set up by Qualcomm in late 2013 that enables gadgets to find, interface, and discuss legitimately with other AllJoyn-empowered items associated with various advancements, for example, Wi-Fi, Ethernet, and conceivably Bluetooth and ZigBee.

- Communication conventions: Once gadgets are associated with a system and they recognize one another, correspondence conventions (a lot of principles) give a typical language to gadgets to convey. Different correspondence conventions are utilized for gadget to-gadget correspondence; comprehensively, they fluctuate in the configuration where information bundles are exchanged. There are progressing endeavors to distinguish conventions more qualified to IoT applications. Toward that end, we prior talked about the points of interest and confinements of the Constrained Application Protocol, a correspondence convention lighter than other prominent conventions, for example, HTTP [3].

- Data total gauges: Data gathered from various gadgets come in various organizations and at various examining rates—that is, the recurrence at which information is gathered. One lot of information total apparatuses—Extraction, Transformation, and Loading (ETL) instruments—total, procedure, and store information in a configuration that can be utilized for examination applications. Extraction alludes to gaining information from numerous sources and different configurations and afterward approving to guarantee that solitary information that meets a measure is incorporated. The change incorporates exercises, for example, part, consolidating, arranging and changing the information into an ideal. Arrangement—for instance, names can be part into first and last names, while addresses can be converted into city and state group [4]. Stacking alludes to the way toward stacking the information into a database that can be utilized for investigation applications.

1-2 Augmented behavior

In its least complex sense, the idea of "enlarged conduct" is the "doing" of some activity that is the consequence of all the previous phases of the esteemed circle—from defecting to the investigation of information. Expanded conduct, the last stage insider savvy, restarts the circle since activity prompts the production of information when designed to do as such. There is a flimsy line between enlarged insight and increased conduct [5]. For our motivation, increased insight drives educated activity, while enlarged conduct is a discernible activity in reality. As a down to earth matter, enlarged conduct discovers articulation in any event three different ways:

- Machine-to-machine (M2M) interfaces:

M2M interfaces allude to the arrangement of innovations that empower machines to speak with one another and drive activity. In like manner vernacular, M2M is frequently utilized conversely with the IoT. For our motivations, however, the IoT is a more extensive idea that incorporates machine-to-machine and machine-to-human (M2H) interfaces, just as emotionally supportive networks that encourage the administration of data in a manner that makes esteem [6].

- Machine-to-human interfaces:

We talk about M2H interfaces with regards to singular clients; business clients of M2H interfaces are examined in the following component, hierarchical substances. In light of the information gathered and algorithmic figurings, machines can possibly pass on suggestive activities to people who at that point practice their attentiveness to take or not to make the prescribed move. With human association, the IoT talk shifts into a marginally extraordinary heading, toward conduct sciences, which is unmistakable from the information science that embodies the first four phases concentrated on making, discussing, collecting, and breaking down the information to determine significant bits of knowledge.

Figure. 1. Examples of M2M and M2H applications

2 THE IOT TECHNOLOGY ARCHITECTURE

2-1 Overview

The Information Value Loop can fill in as the foundation of an association's way to deal with IoT arrangement improvement for potential use cases. To change thoughts and ideas talked about before in the report into the solid structure squares of an answer, we set a start to finish IoT innovation engineering to direct IoT arrangement improvement. This engineering joins system choices for execution exercises [7]. It can fill in as a playbook for building up the vision for an IoT arrangement and for changing over that vision into unmistakable reality. Design for controlling the advancement and organization of IoT frameworks comprises of the accompanying perspectives:

- Business: This view characterizes the vision for an IoT framework and spreads perspectives, for example, rate of profitability, offer, consumer loyalty, and upkeep costs.
- Functional: The linchpin of the reference engineering, this view traverses modules that oblige abnormal state data course through the framework. It contains the utilitarian layers for information creation, preparing, and introduction.
- Usage: This view indicates how the reference model acknowledges the key abilities wanted in a utilization situation. It might incorporate the nitty gritty use case depiction, client voyage, and necessities.
- Implementation: A specialized portrayal of use situation sending, this view fuses the advancements and framework segments required to execute the capacities recommended by the use and practical perspectives.
- Specifications: Finally, this view catches the total IoT stack to be conveyed. It incorporates point by point specialized particulars for the work out of the arrangement.

3 WHY IS A STANDARDIZATION FOR IOT NEEDED

Similarly, as with most troublesome innovations, IoT arrangements are created by a wide scope of suppliers advancing their exclusive methodologies. This can seriously affect interconnectivity. With the extension of the IoT, there is currently an expanded requirement for interoperability of a wide range of frameworks and stages [8]. This must be accomplished through wide International Standards. Such Standards will set up shared conviction seeing subjects, for example, wording (ISO/IEC 20924, Definition and vocabulary for the Internet of Things) or reference models (ISO/IEC 30141, Internet of Things Reference Architecture) that will help item engineers convey an interoperable biological system. Without such Standards, the IoT will be stuck on confined islands and this will hamper its extension.

3-1 Sensors and IoT

Fundamentally, a sensor is a gadget that reacts to a physical boost, for example, heat, light, stable, weight, attraction or movement and transmits data that is utilized to create an activity, for example, on/off, open/close or begin/stop. The guidelines that guide sensors and their work are a vital piece of numerous IEC International Standards, for instance, the IEC 61508 Functional Safety arrangement created by IEC Subcommittee (SC) 65A; or IEC 61757 on fiber optic sensors created by IEC SC 86C. IEC Technical Committee (TC) 47 gets ready productions that identify with semiconductor gadgets, including sensors. IEC TC 76 covers sensors that depend on lasers and the rundown could go on.

3-2 Nanotechnology and the IoT

Sensors are modest, however, they are currently getting much littler. Two-dimensional materials, for example, graphene permit further scaling down of sensors; two-dimensional on the grounds that they are just a single iota thick. Work on graphene and carbon nanotube materials is facilitated in IEC TC 113. Graphene is a perfect material for sensors because of its alluring warm and electrical conductivity, electrical properties and an enormous surface to volume proportion.

3-3 Big Data and the cloud

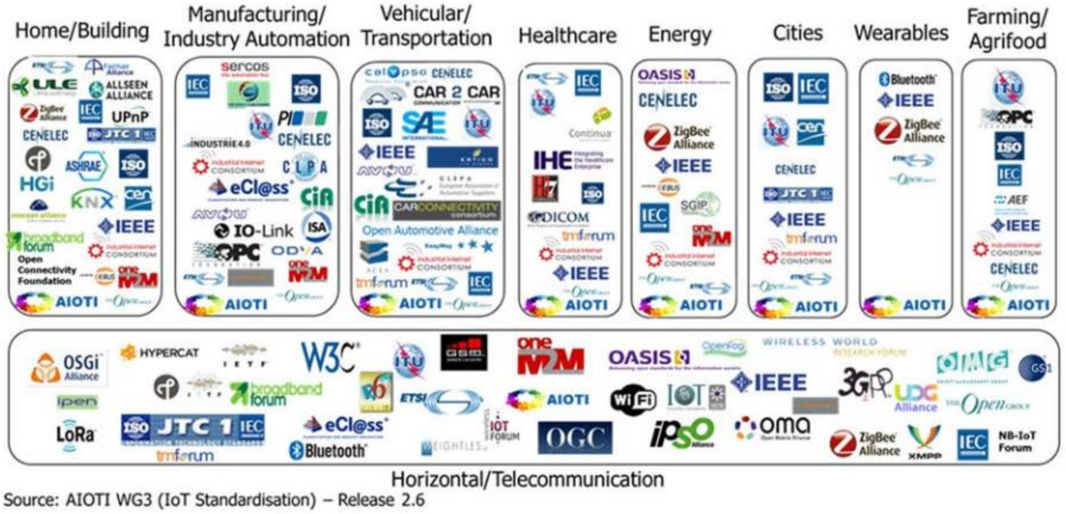
While sensors gather information self-rulingly, they need processors to haul out the data contained in this information. The availability of progressively moderate registering force is a key component in comprehending these undeniably huge information streams. The move to computerized has monstrous repercussions for information. We are encompassed by a blast of information. Specialists gauge than 90% of the world's information has been produced somewhere in the range of 2013 and 2016. As digitization proceeds, information age quickens. As information develops, we need better approaches to make a request from expanding disorder and concentrate important, noteworthy data. The IEC and ISO cooperate in ISO/IEC Joint Technical Committee (JTC) 1/WG 9 on Big Data to scope the job of institutionalization here and distinguishing holes that should be tended to. Though information used to be only put away on gadgets, a lot of it is currently kept in the cloud. This offers a piece of close boundless information stockpiling limit that can be gotten to from anyplace [9]. The IEC by means of ISO/IEC JTC 1/SC 38 works in addition to other things on Standards for distributed computing and appropriated stages.

3-4 Cybersecurity and IoT

Big Data opens numerous new market openings yet it additionally creates new dangers including that of digital assaults or inquiries around the responsibility for just as protection concerns. Specialists feel that the most concerning issue confronting IoT won't be the correspondence between gadgets or the gathering and capacity to share information yet rather the protected keeping of information [10, 11, 12]. Worldwide weakness to vindictive acts on the internet is developing. The inability to verify one gadget can directly affect numerous others and there is an expanding need to apply solid security strategies to keep away from that dangers are passed onto progressively significant frameworks. The abuse of digital vulnerabilities of framework frameworks is turning into an expanding risk to business and society's general security. The IEC has distributed more than 200 International Standards that in all respects legitimately address cybersecurity and security of wellbeing, business, and basic framework frameworks [13, 14, 15]. The IEC Conformity Assessment Systems are likewise dynamic in cybersecurity; the IEC Conformity Assessment Board Working Group 17 is centered around home robotization, brilliant gadgets just as restorative gadgets. ISO/IEC 27001 and ISO/IEC 27002 give a typical language to address administration, hazard and consistency issues identified with data security. ISO/IEC 27031 and ISO/IEC 27035 assistance associations to successfully react, diffuse and recoup from digital assaults [16, 17]. There are additionally ISO/IEC Standards that guarantee the insurance of by and by recognizable data, characterize encryption and mark instruments that can be coordinated into items and applications to secure online exchanges, Visa uses and put away information.

4 THE IOT STANDARDS LANDSCAPE

A portion of the models applies to explicit verticals. Likewise, see figure 2. A portion of these guidelines apply crosswise over verticals and it isn't the focal point of the present archive to rehash the data however to make the examination obvious and feature its significance to the specific vertical if pertinent.


Home/Building
Manufacturing/ Industry Automation
Vehicular/ Transportation
Healthcare
Energy
Cities
Wearables
Farming/ Agrifood
Horizontal/Telecommunication

Source: AIOTI WG3 (IoT Standardisation) – Release 2.6

Figure. 2. IoT SDOs and Alliances Landscape (Vertical and Horizontal Domain)

There are a few Standard Landscapes in every application in Iot, in beneath we referenced a portion of the normal and primary explicit Landscapes in Communication and Connectivity, IoT Architecture, Security and Privacy that appeared in Tables 1, 2, 3 [10, 11, 12].

Table 1COMMUNICATION AND CONNECTIVITY STANDARDS LANDSCAPE

SDO	Standards
3GPP multi-purpose	ETSI TS 123 002 (network architecture) ETSI TS 123 401 (Packet Radio Service) ETSI TS 136 300 (Radio Access Overall description)
3GPP for MTC (Machine Type Communications)	LTE- (LTE for MTC) ,EC-GSM, NB-IoT
Bluetooth	Bluetooth BR/EDR (basic rate/ enhanced data rate) Bluetooth Low Energy (BLE)
DASH 7 Alliance	DASH 7 (ISO 18000-7)
EnOcean Alliance	ISO /IEC 14543-3-10: Wireless Short-Packet (WSP)
ETSI	Terrestrial trunked Radio (T ETRA); ETSI EN 300 392
ETSI DECT	ETSI TS 102 939-1 (DECT ULE phase 1) ETSI TS 102 939-2 (DECT ULE phase 2) Digital Enhanced Cordless Telecommunications (DECT); Ultra Low Energy (ULE); Machine to Machine Communications; Part 1: Home Automation Network (phase 1 and 2) ETSI EN 300 175 (DECT; Common Interface (CI) multi-part specification)
IEEE 802 LAN/MAN	IEEE 802.11 (WLAN) IEEE 802.15.4 (LR-WPAN)
IETF 6lo	Definition of Managed Objects for 6Lo WPAN s (IET FRFC 7388) 6Lo WPAN - GHC (IET FRFC 7400) Transmission of IPv 6 Packets over Recommendation IT U - TG. 9959 Networks (IET F R FC 7428) Low Energy (IET F R FC 7668) Ipv 6 over BLUETOOTH

Table 2 IOT ARCHITECTURE STANDARDS LANDSCAPE

SDO	Standards
AIOTI	IoT high-level architecture (AIOTI WG3)
IEEE	IEEE P2413 (Standard for an Architectural Framework for the Internet of Things (IoT))
Industrial Internet Consortium (IIC)	Industrial Internet Reference Architecture (IIRA) tetrarch .tr.00 1
ISO /IEC JTC1	Information technology - Internet of Things Reference Architecture (IoT RA) (under development)
ITU-T	Recommendation ITU-TY. 2060 "Overview of the Internet of Things " Recommendation ITU-TY. 2068
oneM2M	ETSI TS 118 101, Function al_Architecture
Future Internet Public-Private Partnership (FI-PPP)	Fiware

Table 3 SECURITY AND PRIVACY STANDARDS LANDSCAPE

SDO	Standards
3GPP	ETSI TS 133 220 Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture Describes the security features and a mechanism to bootstrap authentication and key agreement for application security from the 3GPP AKA mechanism. ETSI TS 133 102 (Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 9)) ETSI TS 121 133 (Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements) ETSI TS 133 120 (Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives.)
ETSI DECT	ETSI EN 300 175-7
Hypercat	Hypercat3 specification
IEEE	IEEE 2600-2008
IETF	IETFR FC 5246
IETF	Oauth Authentication and Authorization for Constrained Environments (ACE)
ISO /IEC	ISO /IEC 27000-series ISO /IEC 29100:2011 provides a privacy framework
oneM2M	ETSI TS 118 103

5 CONCLUSION

This paper has displayed an overview of late advances and principles for IoT. Since early IoT frameworks have been created in a vertical administration model, interoperability among different administration areas is a major issue in an ongoing day. A great deal of those conventions has been created and institutionalized by ISO, IEC, IETF, IEEE, ITU, and different associations while a lot more are still being developed. The dialog was brief because of the enormous number. Subsequently, references for additional data have been given. The point of this paper is to give knowledge to engineers and specialist organizations about options for various layers of conventions in IoT and how to pick among them.

REFERENCES

[1] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. McCann, and K. Leung, “A survey on the IETF protocol suite for the internet of things: standards, challenges, and opportunities,” in IEEE Wireless Communications, vol. 20, no. 6, 2013, pp. 91-98.

[2] J. Granjal, E. Monteiro, and J. Sa Silva, “Security for the internet of things: A survey of existing protocols and open research issues,” in IEEE Communications Surveys Tutorials, vol. 17, no. 3, 2015, pp. 1294-1312.

[3] H. Hosseinian and H. Damghani, “Smart home energy management, using IoT system,” in *5th Conference on Knowledge Based Engineering and Innovation (KBEI)*, IEEE, 2019.

[4] H. Damghani, H. Hosseinian, and L. Damghani, “Overview of security aspects for LTE and LTE-A networks,” in *14th Media Technology Conference,* Islamic Republic of Iran Broadcasting, Tehran, Iran, December 2017.

[5] H. Damghani, “RFID Technology: Benefits and Applications,” *Monthly Journal of Transportation and Development*, vol. 36, pp. 70–73, August 2010.

[6] H. Damghani, H. Hosseinian, and L. Damghani, “Investigating attacks to improve security and privacy in RFID systems using the security bit method,” in *5th Conference on Knowledge Based Engineering and Innovation (KBEI),* IEEE, 2019.

[7] K. Naito, “A Survey on the Internet-of-Things: Standards, Challenges, and Future Prospects,” Journal of Information Processing, vol. 25, pp. 23–31, Jan 2017.

[8] European Telecommunications Standards Institute, “Smart M2M; IoT Standards landscape and future evolutions,” European Telecommunications Standards Institute, ETSI TR 103 375, V1.1.1, 2016. [Online]. Available: http://www.etsi.org.

[9] IEEE. Ieee 802.15: Wireless personal area networks (pans), available from ⟨https://standards.ieee.org/about/get/802/802.15.html⟩.

[10] ZigBee Alliance: Zigbee 3.0, available from ⟨http://www.zigbee.org/zigbee-for-developers/zigbee3-0/⟩

[11] H. Damghani, L. Damghani, H. Hosseinian and R. Sharifi, “Classification of Attacks on IoT,” in *4th International Conference on Combinatorics, Cryptography, Computer Science and Computation,* November 2019.

[12] L. Damghani, H. Damghani, H. Hosseinian, H. Mohammadnezhad Shourkaei, “Analytics in Internet of Things and BigData,” in *4th International Conference on Combinatorics, Cryptography, Computer Science and Computation*, November 2019.

[13] H. Damghani and L. Damghani, “Security improvement of Common Scrambling Algorithm (CSA) using the encryption extension technique,” in *16th Iran Media Technology Exhibition & Conference (IMTEC2019),* IEEE, 2019.

[14] H. Damghani, H. Hosseinian, and L. Damghani, “Bitcoin through Amateur Radio,” in *4th Conference on Technology In Electrical and Computer Engineering (ETECH2019),* 2019.

[15] H. Damghani, H. Hosseinian, and L. Damghani, “Cryptography review in IoT,” in *4th Conference on Technology In Electrical and Computer Engineering (ETECH2019),* 2019.

[16] H. Hosseinian, H. Damghani, L. Damghani, G. Nezam and H. Hosseinian, “Home appliances energy management based on the IoT system,” *The International Journal of Nonlinear Analysis and Applications,* 2019.

[17] H. Hosseinian, H. Damghani, L. Damghani, E. Kouhi and M. Kouhi, “Asia’s Cities: The way to Going Smart,” *The International Journal of Nonlinear Analysis and Applications,* 2019.