Internet of Things: Concept, Implementation and Challenges*

Nilupulee A. Gunathilake, Ahmed Al-Dubai, and William J. Buchanan

School of Computing, Edinburgh Napier University, United Kingdom

Abstract. Through the technical advancements over five generations, today's digital communication has become much smarter, more intelligent and punctual. This causes a massive amount of continuous data collection in real-time whose analytics are later used to make useful insights, *i.e., prevention of road accidents using vehicular communication applications, fault detection in industrial machineries, etc.* The means of information reception is usually via sensors. This inter-connectivity of communicating things is basically known as internet-of-things (IoT) which will become a wide-spread infrastructure of next-generation networking.

The devices used in the IoT are physically small and resource-constrained, *i.e., low-end processors, small internal capacities, etc.* Also, those are operated in small data rates, usually in kbps. Thus, it is unable to adopt conventional security mechanisms which require high-end computational processing. Meanwhile, the low energy consumption of these networks conducive for green networking requirements offering the planet a sustainable atmosphere.

Due to the wide ranging nature of the subject, existing literature studies often focus on a narrowed-down area. This survey identifies up-to-date information on all IoT related topics, *i.e., technologies, standardisation, liability, regulations, security, etc.*. This will provide a useful reference for beginners in the field for quick overall comprehension.

Keywords: IoT technologies · IoT standards · IoT security · green networking.

1 Introduction

The next generation technology platforms are mainly based on 5G cellular evolution, big data, industrial 4.0, internet, machine-to-machine (M2M) communication and internet-of-things (IoT). In contrast, the IoT further introduces several versions known as industrial IoT (IIoT), internet-of-everything (IoE), internet-of-me (IoM) and web-of-things (WoT) [14]. The IoT is a novel approach which is becoming highly successful in terms of smartness, intelligence, autonomy and portability all over the world and beyond.

* *This work is supported by the research grants from the School of Computing, Edinburgh Napier University.* Any correspondence related to this article can be sent to (nilupulee.gunathilake@napier.ac.uk)

The core of the IoT purpose is to produce useful insights depending on the nature of data gathered. The vision of the IoT involves many emerging technologies such as artificial intelligence (AI), machine learning and blockchain to be specific. Estimations predict that there may be 200 billion connected devices already in 2020 with an economic impact to be $13 trillion per year by 2025 [5]. The evolution of the IoT is known to start from wireless ad hoc networks that allow direct connectivity between the devices through wireless nodes.

IoT promises to be applied from personal use to applications in space, as in,

- **Low power applications**: Intelligent transportation systems (ITS) including vehicular communications (VANET, V2X), smart home/ office/ buildings/ cities/ streetlights/ metering/ logistics, disaster rescue missions and intelligent security systems.
- **Sensor-based applications**: Agriculture, health monitoring via wearable devices, climate and weather monitoring and data analytics, factory automation (*i.e., failure predictions, etc.*), ITS (*i.e., automatic pilot, etc.*), machine-to-machine (M2M) communication, natural disaster/status monitoring (i.e., water length in a dam, etc.)
- **Tactical applications**: Mission-critical military use (*i.e., army ad hoc radios, navy ship area ad hoc networks, etc.*), ad hoc robotics, unmanned aerial vehicle (UAV), explosive hopping mines, space shuttle missions, etc.

Among various wired or wireless choices in the IoT, its data flow is recognised to be automatic, dense, unobtrusive and structured. Therefore, dependable pros and cons may exist in budget (CapEx and OpEx), energy drainage and accuracy of the results. For example, contact tracing mobile apps issued by the UK government for Covid19 pandemic control require each individual's location data in real time. However, turned off phones/GPS or denied permissions by the user would add an unknown tolerance to the produced insight.

1.1 Our Contribution

Innovations and enhancements of IoT applications are greatly being updated. Besides, the opaque transmission of data tends to cause serious privacy violations. For this reason, both professional and non-professional bodies require a thorough awareness of this large area of activity. Available surveys mainly discuss a particular domain, whereas this work summarises up-to-date information of all IoT related topics.

This paper deals with the IoT communication architecture, propagation techniques, status and challenges in standardisation, law and regulations as well as security. We also consider green networking.

2 Internet of Things

IoT is a complex infrastructure that includes sensing, clusters of data from numerous sources and remote monitoring. The interaction of human-to-human or

human-to-computer is not a necessity. The transmission covers four levels: device, edge, fog and cloud, as shown in Fig.1 [7]. The device layer contains sensor nodes. Then sensed data is processed through edge and fog computing up to the cloud where information is saved. The communication is often wireless as well as full duplex.

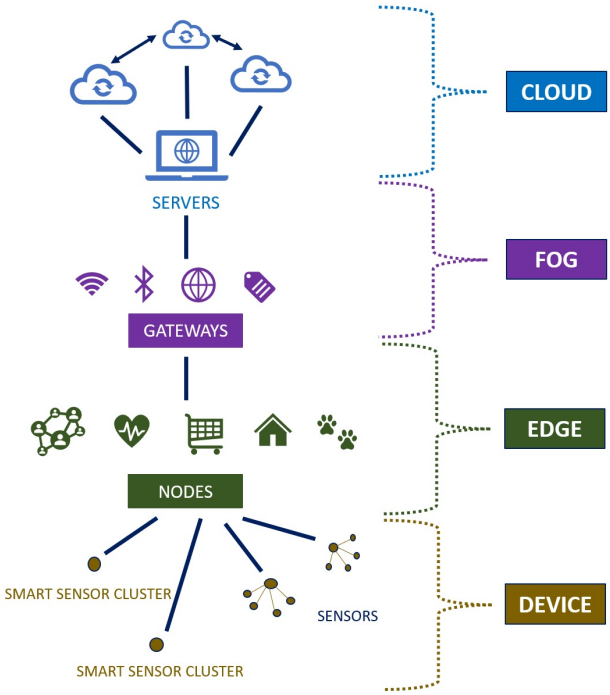

Fig. 1. IoT communication architecture

This extensive area is subjected in different categories to offer the optimised functionalities nationally and internationally. This includes propagation technology development, privacy/safety challenges, standardisation in common platforms technically to avoid translation overheads [13] and law/regulation fixation for liability.

The frequency spectrum used here is the unlicensed ISM (industrial-scientific-medical) band. Depending on future possibilities, the licensed band may be utilised because the existing wired/wireless telecommunication infrastructure operated under the International Telecommunication Union (ITU) regulations also uses IoT benefits.

3 Propagation Technologies

There are numerous transmission protocols used and still being developed that are compatible with efficient IoT communication. Among those, Wireless Fidelity (Wi-Fi), Bluetooth Low Energy (BLE), Narrowband (NB) IoT, Long Range Wide Area Network (LoRaWAN), SigFox, ZigBee and Z-wave are trending.

Wi-Fi is based on the IEEE 802.11 standard that generally consumes 1mW of power. Several versions of it have been introduced subsequently. Their relevant parametric values are in Table 1. The IEEE 802.11p is specifically allocated to vehicular ad hoc networks (VANet) [11], and the standards which have two simple letters after 802.11 are known to be the next generation Wi-Fi enhancements including IEEE 802.11ba in addition [9].

Table 1. Wi-Fi - IEEE 802.11 standard's versions

Wi-Fi	Frequency	Data Rate	Range
IEEE 802.11a	5GHz	6M–54 Mbps	120m
IEEE 802.11b	2.4GHz	1M–11 Mbps	140m
IEEE 802.11g	2.4GHz	6M–54 Mbps	140m
IEEE 802.11n	2.4/5GHz	288M–600 Mbps	250m
IEEE 802.11p	5.9GHz	3M-27 Mbps	1km
IEEE 802.11ac	5GHz	346M–3.466 Gbps	70m
IEEE 802.11ad	60GHz	Up to 6.7Gbps	1-10m
IEEE 802.11ah	900MHz	Up to 347Mbps	1km
IEEE 802.11aj	45/60GHz	-	1km
IEEE 802.11ax	2.4/5GHz	Up to 10.53Gbps	70-240m
IEEE 802.11ay	60GHz	Up to 20Gbps	100m
IEEE 802.11az	60GHz	-	-

BLE is a subversion of generic Bluetooth that is explicitly implemented for power-constrained device-to-device (D2D) communication. Due to the low energy consumption, the battery would gain its lifetime in years. The connection times are in a few milliseconds while the power drainage is in a few microWatts. It has a high data rate, approximately 1Mbps.

NB-IoT was standardised as the Third Generation Partnership Project (3GPP)'s Release 13 in 2016 [20]. It operates on LTE FDD 180kHz frequency band under three modes of operations which are stand-alone, guard-band and in-band.

LoRaWAN is an enhancement of LoRa protocol that is used to establish direct communication in long distances up to several kilometres. With this, network sessions are handled between nodes and gateways as well as end-to-end encryption at the application level. Moreover, *over the air* registration/activation and multicasting are the main advantages of this low power WAN. The general specifications are as in Table 2 [3]

Table 2. LoRaWAN specifications

Parameter	Value
Frequency band	ISM 433MHz ISM 868MHz ISM 915MHz
Data rate	27kbps
Range	Urban 2-5 km Clear LoS 15km
Network topology	Star

Sigfox is a proprietary LPWAN technology operating on ISM 868/902MHz bands. It employs DBPSK and GFSK modulation techniques in a star network topology. Its security mechanisms are tailored via AES-128.

ZigBee is an open standard which is designed to facilitate interoperability between IoT devices due to its affordability, adaptability and deployability. This technology is well suited to sleeping end-devices and energy harvesting applications. It can tolerate up to 65,000 nodes at 250kbps.

Z-Wave is a series of implementations for future proof LPWAN hardware with integrated software tools. It also introduced the SmartStart protocol that empowers pre-configuration of devices to the network by security authorities prior to installation. This evidently reduces time spent on site which would result in minimised CapEx and OpEx as well as maximised RoI. The expected data rates are between 40-100 kbps and it is capable of allocating up to 232 devices in the network [1].

4 Standardisation

The nature of the IoT standardisation process is complex due to its opaque data flow, continually upgrading hardware, software and network functionalities over billions of connected things. To take forward steps in an interoperable, heterogeneous and secured IoT ecosystem, standardisation is a must. For example, unique standards offered by a number of manufacturers would require extra expense in translation to connect a device with another kind of standard [13]. Work is progressing towards accomplishing this need, as described under the following topics, 4.1, 4.2 and 4.3.

4.1 Global Standards Development

The authorities relavent to the case are classified to be Standards Development Organisations (SDO), government agencies and industrial contributors. They mainly consider the openness, transparency, mechanisms, power balance/liability issues and due processes to certify adherence to anticipated procedures [15]. The types of committees involved there are as below;

- **Formally recognised fora**
  ITU, International Organization of Standards (ISO)/International Electrotechnical Commission (IEC), European Telecommunications Standards Institute (ESTI), etc.
- **Global fora/consortia**
  Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), Organisation for the Advancement of Structured Information Standards (OASIS), etc.
- **Small/private consortia**

4.2 Standards for Functionality and Compatibility

This includes consensus-driven efforts, private and proprietary standards. The IETF, ISO/IEC and IEEE are the major partners in this. Technically, a vast area of protocols and technologies is defined to handle proper functionalities in the IoT environment, but further optimisation is essential in order to obtain fewer specific compatible standards. Some of the widely used examples are;

- **Communication / Transport**: *Wi-Fi, BLE, LPWAN, etc.*
- **Data protocols**: *Message Queuing Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), Constrained Application Protocol (CoAP), Websocket, Node, etc.*
- **Device management**: *Technical Report (TR)-069, Open Mobile Alliance Device Management (OMA-DM), etc.*
- **Discovery**: *Physical Web, multicast Domain Name System (mDNS), DNS Service Discovery (DNS-SD), etc.*
- **Identification**: *Electronic Product Code (EPC), uCode, Internet Protocol version 6 (IPv6), Uniform Resource Identifiers (URIs), etc.*
- **Infrastructure**: *6 Low-power Wireless Personal Area Network (6LoWPAN), IPv4/IPv6, Routing Protocol for Low-Power and Lossy (RPL), etc.*
- **Multi-layer frameworks**: *AllJoyn, IoTivity, Weave, Homekit, etc.*
- **Semantic**: *Java Script Object Notation - Linked Data (JSON-LD), Web Thing Model, etc.*

4.3 Standards for Security and Privacy

Security and privacy vulnerabilities mostly depend on a particular operation or application. However, device connectivity to either cloud or fog is an assured task. Thus, the amount of data to be transferred/processed is time-sensitive too. In that case, a quadruple trust, namely, a combination of protection, security, privacy and safety, is the aim of the authorities in their efforts via proper security models, *i.e., blockchain, lightweight cryptography, etc.*

The National Institute of Standards and Technology (NIST) has introduced a cybersecurity framework with five layers, specified as identify, protect, detect, respond and recover. That also includes asset management, access control and detection process to address IoT threats and hazards. Meanwhile, the IEC states in their 62443 release that conformity assessment process and certification thereafter by certification bodies is a promising data safety structure [2].

4.4 Law and Regulations

Transparency, responsibility and liability of IoT data are challenging issues to be addressed due to personal, industrial and governments' overall engagement which could trigger risks individually, locally, regionally and internationally. Hence, power imbalance and possible security breaches must be subjected to introducing or updating law and regulation frameworks specifically for IoT related cybersecurity issues. Some of the considerations in this are [4, 15];

- Evidence-based support to make cost-beneficial assessment/insurance across affected stakeholders
- Application of product liability for IoT services
- Execution of recommended security standards for integrated IoT features and practices
- Enforcement of minimum-security warranties for data and products
- Transitive liability scheme for supply and service chains
- Compulsory disclosure of IoT security breaches meeting certain thresholds
- Penalty based regulations if the security of IoT is ignored or for insecure products and practices

Presently the General Data Protection Regulation (GDPR) brought by the European Union (EU) is implementing strict policies that apply to both personal data and personal-sensitive data in IoT. Besides, ePrivacy regulation of the EU would also smooth up the principles of confidentiality in IoT expansions. The USA mainly follows the Connected Devices Act [12]. Consequently, baseline security standards are required for all connected devices in government that ban the procurement of devices with hardcoded passwords or known weaknesses which are incapable of being updated.

5 Data and Network Security

The most significant difference between the IoT and former internet technology is that the probabilities of threats and hazards are substantially greater because of [8, 19];

- **More points of exposure**: An exponential increase in connected devices, applications, systems, end-users through billions of billions of communication nodes
- **Creation of new self-attack vector**: Every compromised node becomes a new attack point that may remain unnoticed for a while
- **Risen impacts of attacks**: Due to incompatibility among a number of standards, blind spots may be an advantage to attackers
- **New threats form across the stack**: 'More complexity to sort out' means daily forming new threats where continuous attention of security professionals is high priority

Blockchain and lightweight cryptography [6, 7] are the major mechanisms in IoT security. The following formula is used to measure cybersecurity risk [17];

$$CybersecurityRisk = \frac{ThreatLevel \times Probabilityof Attack \times Pointof Exposure}{CybersecurityMeasuresimplemented}$$

IoT security structures exist under four main layers depending on methods of computation and communication atmosphere, as in Figure 1 and Figure 2. It is assumed that the highest percentage of security breaches is possible at the cloud level while it is the minimum at the device level.

- **Device**: Hardware level including the elements of physical security, data at rest, chip security, secure booting, device authentication and its identity via edge processing.
- **Communication**: Connectivity networks via fog computing that cover physical layer, *i.e., Wi-Fi, Ethernet, etc.*, network layer, *i.e., IPv6, Modbus, etc.*, and application layer *i.e., MQTT, CoAP, etc.*, of the OSI model that is extremely prone to man-in-the-middle attacks. This includes access control, firewall, intrusion prevention system (IPS), intrusion detection system (IDS) [16] and end-to-end encryption to be made sufficiently secure.
- **Cloud**: Software backend where received data is analysed, insights are generated and useful actions are performed. At this level, components of data at rest, platform/application integrity verification [18] and unified threat management [10] are matters of concern.
- **Lifecycle management**: Handling of continuous processes to keep sufficient security up-to-date. Hence, risk assessment, activity monitoring, vendor control, user awareness assessment, policies and auditing, updates and patches and secure decommissioning should be maintained [17, 18].

In addition, ***processing data locally whenever cloud storage is not necessary is a suitable security mechanism to lower the risks***, *i.e., VPN*. Methods of data wipe out for compromised devices remotely would be an option to avoid spreading vulnerabilities over the entire network.

6 Green Networking

Green networking is a practice of enhancing energy-efficient networking technologies and products, and optimally minimizing resource use sustainably. Therefore, it is an added advantage of IoT implementations due to its small power consumption and resource limitations. The stack of IoT techniques and procedures that satisfies this scenario is alternatively known as green IoT applications, *i.e., green design, green production, green utilisation and green disposal/recycling.*

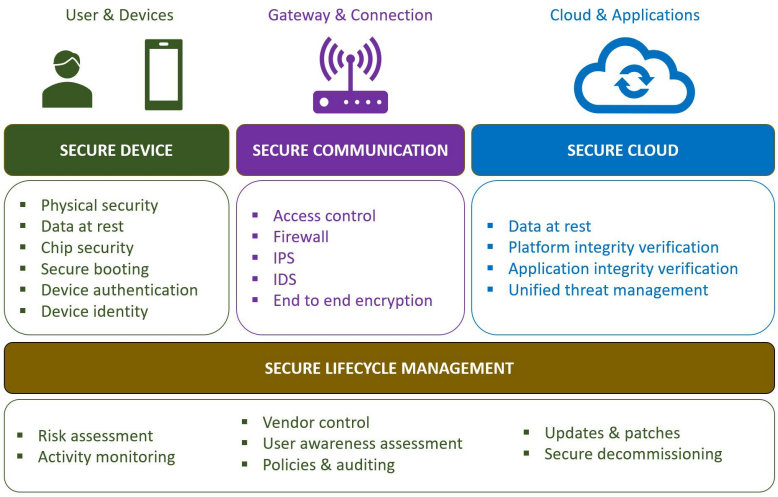

Fig. 2. IoT security architecture

7 Conclusions

IoT is a massive infrastructure in the coming generation that is an integration of billions of resource constraint devices. The devices are operated on low data rates, low onboard memory and usually battery-powered. Special technical enhancements are introduced to tackle these constrained computational functions. For example, MQTT is an IoT supportive data protocol where transmission technologies like BLE, NB-IoT and LoRaWAN handle low power full-duplex communications up to the cloud. In parallel, privacy and data protection complexities emerge due to the opaque nature of IoT data distribution. National and international authorities (*i.e., NIST, ISO/IEEE, the EU, etc.*) are working on introducing and updating legal frameworks for IoT efficiency and liability (*i.e., GDPR, ePrivacy, etc.*) However, adequate IoT security still struggles to provide compatible lightweight primitives to cope with possible and futuristic IoT hazards and threats (*i.e., AI, blockchain and lightweight cryptography*).

References

1. Introduction to Z-Wave SmartStart (Sep 2017), https://www.silabs.com/documents/login/white-papers/introduction_to_z-wave_smartstart_091317.pdf-Accessed:Jan.11,2020
2. IEC 62443-4-1 Security for Industrial Automation and Control Systems (Part 4-1: Secure Product Development Lifecycle Requirements (2018), https://webstore.iec.ch/publication/33615-Accessed:May05,2020
3. LoRaWAN Classes (2020), https://www.thethingsnetwork.org/docs/lorawan/classes.html-Accessed:Apr.01,2020

4. Barrera, D., Molloy, I., Huang, H.: Standardizing IoT Network Security Policy Enforcement (Jan 2018), doi: 10.14722/diss.2018.23007
5. Gremban, K.: Editorial and Introduction to the Issue: Risk and Rewards of the Internet of Things. IEEE Internet of Things Magazine (IoTM) **1 September**(1), 2 (Sep 2018), https://www.comsoc.org/publications/magazines/ieee-internet-things-magazine
6. Gunathilake, N.A., Al-Dubai, A., Buchanan, W.J.: Recent Advances and Trends in Lightweight Cryptography for IoT Security. In: 16th International Conference on Network and Service Management (CNSM 2020) (Nov 2020), http://dl.ifip.org/db/conf/cnsm/cnsm2020/1570662904.pdf
7. Gunathilake, N.A., Buchanan, W.J., Asif, R.: Next Generation Lightweight Cryptography for Smart IoT Devices: : Implementation, Challenges and Applications. In: 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). pp. 707–710 (2019), doi: 10.1109/WF-IoT.2019.8767250
8. Gurunath, R., Agarwal, M., Nandi, A., Samanta, D.: An Overview: Security Issue in IoT Network. pp. 104–107 (Aug 2018), doi: 10.1109/I-SMAC.2018.8653728
9. Haiming, W., Wei, H., Jixin, C., Bo, S., Peng, X.: IEEE 802.11aj (45GHz): A New Very High Throughput millimeter-wave WLAN System. Communications, China **11**, 51–62 (jun 2014), doi: 10.1109/CC.2014.6879003
10. Jadhav, P.: Cloud Unified Threat Management System. International Journal for Research in Applied Science and Engineering Technology **6**, 1712–1715 (04 2018), doi: 10.22214/ijraset.2018.4288
11. Jiang, D., Delgrossi, L.: IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments. pp. 2036–2040 (Jun 2008), doi: 10.1109/VETECS.2008.458
12. Kenneally, E.: The TTPs of Privacy and Security of the IoT. IEEE Internet of Things Magazine (IoTM) **1 December**(2), 8–11 (Dec 2018), https://www.comsoc.org/publications/magazines/ieee-internet-things-magazine
13. Kranz, M.: Why Industry Needs to Accelerate IoT Standards. IEEE Internet of Things Magazine (IoTM) **1 September**(1), 14–18 (Sep 2018), https://www.comsoc.org/publications/magazines/ieee-internet-things-magazine
14. Lueth, K.L.: Why the Internet of Things is called Internet of Things: Definition, History, Disambiguation. IoT Analytics (Dec 2014), https://iot-analytics.com/internet-of-things-definition/
15. Marcus, J.S.: Liability: When Things Go Wrong in an Increasingly Interconnected and Autonomous World (A European View). IEEE Internet of Things Magazine (IoTM) **1 December**(2), 4–5 (Dec 2018), https://www.comsoc.org/publications/magazines/ieee-internet-things-magazine
16. Padraig, S.: Understanding IoT Security – Part 1 of 3: IoT Security Architecture on the Device and Communication Layers (Nov 2016), https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/-Accessed:Jul.28,2020
17. Scully, P.: Five Things To Know About IoT Security (Nov 2017), https://iot-analytics.com/5-things-to-know-about-iot-security/-Accessed:Jul.27,2020
18. Scully, P.: Understanding IoT Security – Part 2 of 3: IoT Cyber Security for Cloud and Lifecycle Management (Jan 2017), https://iot-analytics.com/understanding-iot-cyber-security-part-2/Accessed:Jul.29,2020
19. Sundar, S., Subramanain, S.: Security Stipulations on IoT Networks, pp. 289–306 (Jan 2018), doi: 10.1007/978-3-319-70688-7_12
20. Violette, M.: Standards Matters. IEEE Internet of Things Magazine (IoTM) **1 December**(2), 6–7 (Dec 2018), https://www.comsoc.org/publications/magazines/ieee-internet-things-magazine