# Architecture and Challenges of Industrial Internet of Things

Subjects: Computer Science, Hardware & Architecture | Engineering, Industrial

Contributor: Soo Fun Tan

The inherent complexities of Industrial Internet of Things (IIoT) architecture make its security and privacy issues becoming critically challenging. Numerous surveys have been published to review IoT security issues and challenges. The studies gave a general overview of IIoT security threats or a detailed analysis that explicitly focuses on specific technologies. However, recent studies fail to analyze the gap between security requirements of these technologies and their deployed countermeasure in the industry recently. Whether recent industry countermeasure is still adequate to address the security challenges of IIoT environment are questionable.

Keywords: Industrial Internet of Things (IIoT) ; IoT architecture and networks ; security and trust

## 1. Introduction

The emergence of the Industrial Internet of Things (IIoT) acts as a new network paradigm that has transformed traditional capturing, collecting, exchanging, processing, and storing data in the industry. IIoT goes beyond the typical consumer devices, people-to-people (P2P) and people-to-machine (P2M) communication networks associated with the IIoT. IIoT consists of billions of “things” intelligently connected via distributed communication networks, such as machine-to-machine (M2M) communication. These “things” ranging from ultra-efficient sensors and actuators, automation devices, embedded systems, heavy machines to high-performance gateways, with real-time data analytics always present.

In most cases, these “things” are uniquely identified by a variety of addressing schemes, includes electronic product code (EPC), ubiquitous code (ucode) and media access control (MAC) and Internet protocol (IP) address. IIoT promises a transformative future for businesses and governments, including intelligent automation, smart factories, intelligent healthcare, smart homes, smart cities, and intelligent transportation. IIoT’s inherent complexities introduce several security challenges and privacy risks. Several surveys and reviews on analyzing IoT and IIoT security threats and privacy challenges have been published over the last decade. These existing reviews and surveys are chronologically summarised in **Table 1**.

**Table 1.** Chronological summary of previous surveys in the IoT and IIoT security.

| Year | Reference | S | I | G | O | Focuses |
|---|---|---|---|---|---|---|
| 2010 | Atzori et al. [1] | √ | √ |  | √ | Data integrity and privacy issues specifically on wireless technologies: RFID and WSN |
|  | Weber [2] |  |  |  | √ | Limited to address data and privacy legislation of the IoT and RFID |
| 2012 | Miorandi et al. [3] | √ | √ |  | √ | A general overview of data confidentiality, privacy and trust specifically on distributed intelligence, communication and identification technologies |
| 2013 | Zhao and Ge [4] |  | √ |  | √ | A brief discussion of security attacks and measurements based on three-layer IoT architecture (perception layer, transport layer and application layer) |
| 2014 | Ziegeldorf et al. [5] |  |  |  | √ | A general overview of IoT privacy threats and challenges |
|  | Jing et al. [6] |  | √ | √ | √ | Analyze the cross-layer heterogenous and security issues of three-layer IoT architecture (Perception layer, transport layer and application layer) and focuses specifically on WSN and RFID |

| Year | Reference | S | I | G | O | Focuses |
|---|---|---|---|---|---|---|
| 2015 | Fremantle and Scott [7] | √ | √ |  | √ | Middleware systems and their security properties, as well as a very brief discussion on future works |
|  | Granjal et al. [8] |  | √ |  | √ | IoT communication protocols and technologies specifically on MAC and Physical layers |
|  | Nguyen et al. [9] | √ |  |  | √ | IoT security protocols and key distribution specifically on WSN |
| 2016 | Airehrour et al. [10] | √ | √ |  | √ | Secure routing protocols and trust models |
|  | Qin et al. [11] | √ |  |  | √ | Review IoT from a data-centric perspective, specifically on RFID |
| 2017 | Loi et al. [12] | √ | √ |  | √ | Comprehensive security analysis on consumer IoT Devices |
| 2018 | Fernández-Caramés et al. [13] |  | √ |  | √ | Blockchain-based IoT application |
| 2019 | Hassija et al. [14] | √ |  |  | √ | Studies on the relationship between IoT application and related technologies: blockchain, machine learning, fog and cloud computing |
|  | Berkay et al. [15] | √ |  |  | √ | Security analysis of IoT programming platforms |
|  | Tabrizi and Pattabiraman [16] | √ |  |  | √ | Design-level and code-level security analysis on IoT devices |
| 2020 | Amanullah et al. [17] | √ | √ |  | √ | Comparative analysis on the relationship of IoT security, deep learning and big data technologies |
|  | Lao et al. [18] | √ | √ |  | √ | A review on blockchain-based IoT architecture |
|  | Joao et al. [19] | √ |  |  | √ | A general review on threat models and attack path of IoT |
| 2021 | Polychronou et al. [20] | √ | √ |  |  | Software attacks targeting hardware vulnerabilities and deep learning detection mechanisms in IIoT |
|  | Gaspar et al. [21] |  | √ |  | √ | A general IoT technologies review on Portugal’s Agro-Industry |
|  | Wu et al. [22] | √ |  |  | √ | Relations between machine learning and blockchain in IIoT |
|  | Latif et al. [23] | √ |  |  | √ | A general review on blockchain-based decentralized IIoT security |

In 2010, Atzori et al. [1] and Weber [2] initiated the studies of IoT security issues. Atzori et al. [1] briefly discuss IoT’s security challenges and privacy issues, particularly in RFID and WSNs. Weber [2] focuses on the security requirements, privacy legislation and personal data protection of the IoT and RFID. Miorandi et al. [3] provided an overview of IoT’s data confidentiality, privacy, and trust issues. Subsequently, Ziegeldorf et al. [4] gave a detailed discussion on privacy threats and challenges of IoT. Zhao and Ge [5] discussed security issues from the IoT architecture perspective and divided IoT into perception, transport, and application layers. Then, Jing et al. [6] further conducted a comprehensive analysis of each layer’s features, security issues, and corresponding solutions. After that, the discussion of IoT security is nailed down on the specific technologies and scope. The study of Fremantle and Scott [7] focuses the analysis on the middleware of IoT security. Granjal et al. [8] centralized on the security of IoT communication protocols, includes physical and medium access control (MAC) layers, IPv6 over low power wireless personal area network (6LoWPAN), routing protocol for low power and lossy networks (RPL). Nguyen et al. [9] focus on the security of IoT and WSN communication protocols and their attack-resistant solutions. Subsequently, Airehrour et al. [10] gave a detailed security analysis of IoT routing protocols, particularly in low-power and lossy networks (LLN). Then, Qin et al. [11] briefly discussed IoT security from a data-centric perspective. Loi et al. [12] directed to analyze consumer IoT devices. Fernández-Caramés et al. [13] and Lao et al. [18] review the adaptability of blockchain in securing IoT applications and architecture. Hassija et al. [14] focus on discussing the security of IoT applications. Berkay et al. [15] and Tabrizi and Pattabiraman [16] directed to review the IoT security from a programming platform and code-level perspective. Amanullah et al. [17] discuss the relationship between deep learning, IoT security and big data technologies. Joao et al. [19] gave a general review of threat models and attack paths of IoT.

Recent IIoT surveys have primarily focused on the general IoT domain rather than the IIoT domain. They either provided a general overview of IoT security [1][2][3][4][5][10][11][19], or a detailed security analysis limited to specific IoT technologies or a particular layer of IoT architecture [6][7][8][9][12][15][16]. In addition, multiple surveys focused on exploring the relationship between IoT security and blockchain technologies [13][14][17][18]. Survey directions have lately been directed to be hammered down in the IIoT domain [20][21][22][23][24]. Deep learning in IIoT threat detection [20][22] and decentralised blockchain technologies [22][23] are the focus of these IIoT security surveys. However, none of them performs comprehensive security analysis on IIoT architecture and its recent industry solutions. Whether these deployed security solutions in the industry are still adequate to be adapted to secure IIoT architecture are questionable. The contributions of this article are:

- The difference between conventional systems and IIoT security concerns are summarized. Decentralized security approaches with high scalability, high interoperability, lightweight, and secure data processing have urged to address the high heterogeneity of “things,” high volume, and variety of collected sensor data, as opposed to conventional security systems focused on a centralized approach.

- Unlike recent IIoT architectures [24][25][26][27] that (i) focused on specific industries: aviation industry [25] and smart manufacturing [27], and (ii) targeted on particular technologies: M2M communication [24], green-aware multi-task scheduling [26] and 5G technology [27], we generalized the IIoT architecture into a four-layer architecture to cope with a wide of industry technologies and standards.

- Subsequently, we classify the recent IIoT technologies and standards into the proposed four-layer IIoT architecture

- The IIoT security requirements are further defined with the CIA+ model, includes confidentially(C), integrity(I), authentication(A), authorization and access control (A) and availability (A).

- A comprehensive end-to-end security analysis was conducted based on the defined IIoT CIA+ model. Subsequently, a fine-grained review on recent industry technologies and standards in each layer of the proposed IIoT architecture. The identified security risks and threats of these industry technologies, their deployed security countermeasures and future research works are summarized

- Lastly, we enumerate the open security challenges of IIoT and future research opportunities.

The rest of this article is organized as follows. Section 2 investigate the characteristic of IIoT, highlights and report the difference between conventional systems and IIoT security concerns. Section 3 review the recent works of IIoT architecture and propose an IIoT security architecture based on the ITU-T Y.2060 IoT reference model [20], consisting of four layers: device layer, transport and network layer, processing layer and application layer. Then, we classify the recent industry technologies and standards into the proposed IIoT security architecture. Subsequently, Section 4 presents a comprehensive end-to-end security analysis on each layer of IIoT architecture by using the CIA+ model. The security risks and threats of each industry technology and their deployed security countermeasure, the gaps of today’s deficiency, and ongoing challenges are reported. Section 5 discusses the open security challenges, privacy issues and future research opportunities of IIoT. Finally, Section 6 concludes.

## 2. IIoT Security Challenges and Concerns

The discussion of IIoT can be traced back to the connection between the physical world and ubiquitous “things” via the Internet during the early 1990s [28]. While IIoT was still in its infancy growth stage, these definitions’ scope is framed by different business interests and industry application scenarios [29][30][31][32][33]. For example, IETF and IEEE definitions are bounded by sensing technologies such as RFID and sensors [29][30], whilst the W3C expound the IoT with the Word Wide Web ecosystems [31]. IoT’s vision is to enable the connection of any “things” anytime. In most industry cases, we concluded that these “things” are associated with three fundamental characteristics: heterogeneity, unique identities and connectivity.

Along with the growth of IIoT for supporting industries, IIoT security and privacy issues have become more challenging. These security challenges inherit the conventional systems issues such as the advanced persistent threat (APT) and are further exacerbated by the complexity of the newer IIoT associated characteristics such as high heterogeneity, large scale of “things”, and cyber-physical systems. **Table 2** further summarises the difference between conventional systems and IIoT security concerns.

**Table 2.** The difference between conventional systems and IIoT security concerns.

| Concerns | Conventional System | IIoT |
|---|---|---|
| **Connected Nodes/Devices** | **Small to medium volume within the local networks** | **Billions of sensor nodes, actuators and automation devices connected** |

| Concerns | Conventional System | IIoT |
|---|---|---|
| Communication Networks | Homogenous | Heterogeneous |
| System Scalability | Optional | High scalability<br>The design of IIoT security systems should consider the identification and authentication of an enormous scale of "things", scalability of communication networks and security key distribution and revocation issues in future |
| System Interoperability | Optional | High interoperability Diverse security mechanisms and defence systems over the distributed networks must be standardized and compatible with each other to communicate, exchange and process data securely |
| Collected Data Types | Unified encoding scheme and data format, structured data | Confluent with the terms of "big data" characteristic:<br>• High volume (terabytes–zettabytes),<br>• High variety (diverse encoding scheme and format, structured data, unstructured data, semi-structured data, quasi-structure data) |
| Data Processing Model | Moving data to process, moderate speed | Moving processing to data. In most industrial cases, high velocity necessitates real-time analytical processing |
| Security and Privacy Concerns | Data-at-rest<br>Data-in-memory<br>Data-in-transit | Data-at-rest<br>Data-in-memory<br>Data-in-transit<br>Data-in-transform |
| Authentication and Access Control Mechanisms | Centralized Approach | Distributed, decentralized approach<br>Lightweight scheme |

The high heterogeneity of "things" on a large scale implicates the interoperability issues of cross-network communications, cyber-physical systems and IIoT enabled-technologies integration. The intricate maze of interoperability issues arises when: (i) heterogeneous devices and sensor nodes are identified with different naming and addressing schemes; (ii) exploit different data structures and formats; and (iii) communicate through different security protocols with varying requirements of the network (e.g., reliability, communication cost, latency and bandwidth) and integrated to provide a plethora of service applications. The question of whether these conventional security mechanisms and defence systems can be further integrated and standardized universally in resolving IIoT security complexities remains unanswered.

When there is a large scale of "things" (e.g., sensors in the aviation industry that consistently capture engine and aircraft health information during a flight) or diverse "things" in smart factories and manufacturing (e.g., sensors, edge devices, and smart grid) that collaborate to generate and exchange data continuously, these generated data from cyber-physical systems always come in big data flavour [17]. The data come in high volume and wide variety (e.g., structured, unstructured, quasi-structured, and semi-structured data), which need to be processed at a high velocity or analyzed nearly real-time, resulting in conventional data processing mechanisms being complicated or too expensive to scale and handle them efficiently.

As conventional data processing systems mainly were built-in houses, centralized management, and typically worked within the organization boundaries with a finite number of connected devices and users; therefore, security and privacy issues were not a concern. However, security protection and defences mechanisms are significantly different in the era of IIoT. Collected sensors data are locally processed and analyzed by IIoT gateway or automation system before sending to a centralized cloud platform for remote monitoring and post-analysis. The scalability of the existing security mechanisms to authenticate, fine-grained access control on massive IIoT resources has drawn the industry and researcher's attention to move forward into a decentralized approach. Subsequently, more lightweight and highly efficient encryption schemes have been proposed recently to protect the tiniest "things" of IIoT, such as edge devices, sensor nodes and WSNs.

## 3. IIoT Architecture

### 3.1. Overview of IoT and IIoT Architecture

The origins of IIoT architecture can be traced back to the early designs of IoT architecture. In 2011, Ning and Wang [34] proposed a future IoT architecture called a U2IoT model. The U2IoT architecture works similar to a human nervous system that consists of unit IoT and ubiquitous IoT. The unit IoT serves as a local unit based on the man-like nervous model and is responsible for handling and managing diverse local IoTs. The ubiquitous IIoT follows the blueprint of social organization framework architecture and is responsible for integrating, managing, and controlling the collaboration among multiple IoT units across the industry, nationwide and worldwide. On the other hand, Guinard [35] worked on the concepts of web of things (WoT) by proposing an architecture that integrates the connection of "things" to the existing web services via existing web technologies. The proposed WoT architecture consists of five layers, includes accessibility, findability, sharing, composition and application layers. Subsequently, Gomez and Lopez [36] extended the WoT concepts into a hybrid distributed IoT architecture that consists of two distinct resource-oriented approaches: WoT and Tripe Space. WoT underlying a hypertext transfer protocol (HTTP) to interconnect the IoTs in the world wide web. Tripe Space applies semantic web protocol to exchange machine-processable data among the heterogeneous devices in the distributed local shared space. Vernet et al. [37] further customized the WoT architecture into the Smart Grid domain. Meanwhile, Olivier et al. [38] and Qin et al. [39] proposed another IoT architecture based on software defined networks (SDN) that consists of three layers: infrastructure layer with interconnecting network devices; control layer that comprises of SDN controllers; and an application layer that includes the applications for configuring the SDN. On the other hand, several research projects such as IoT-A [40], iCore [41], Sensei [42], and COMPOSE [43] have proposed a reference architecture of IoT at a high abstraction level.

A step closer to real-world industry implementation, several researchers [44][45][46][47][48] and vendors (i.e., Finnode, ThingWorx and Xively) use cloud technologies to tackle the IIoT heterogeneity issues and scalability services. These cloud-centric IIoT architectures use a centralized or decentralized cloud platform to process and manage the aggregated data from heterogeneous networks such as RFID, WSN, and body area network (BAN). These cloud-based IIoT platforms also provide API interfaces for industries to develop their IIoT applications. Researchers [49][50][51] recently attempted to integrate blockchain technologies in solving the decentralized issues of cloud-based IIoT architecture. Whether these blockchain-based architectures are practicable to support a large scale of things with their constrained resources in real-world industry implementation needs to be further investigated.

Generally, the initial widely accepted IIoT architecture is constructed based on the three-layer architecture [6][52], namely the perception, network, and application layers. The perception layer consists of the "things" identification and sensing technologies to collect and exchange the data. The network layer enables the communication and data transmission between the perception layer and the application layer. In most cases, it also involves data aggregation and curation process. Lastly, the application layer confluxes the data aggregated and virtualises the analysed result based on society, business and government demands. Different business interests reflect various IIoT applications for this layer, such as smart cities, intelligent health and smart transport. As three-layer architecture confronted the interoperability and scalability problem to well-suit into existing Internet and telecommunication networks, Wu et al. [53] extended the three-layer architecture into five-layer architecture by proposing a new business layer that resides on the top of the application layer and further dividing the previous network layer into processing layer and transport layer. The transport layer is responsible for transmitting the data generated from the perception layer into the processing layer. The processing layer focuses on processing, storing, and performing analytical works based on the application layer's demand. While the application layer consists of diverse IIoT applications customized to each industry requirement, the business layer monitors these applications' release and charging, conducts research on business and profit models, and controls privacy issues. Subsequently, ITU [52] proposed an IIoT reference architecture that consists of four layers: device layer, network layer, service and application support layer and application layer. The device layer is responsible for capturing and uploading data directly or indirectly via communication networks or gateway protocol, such as controller area network (CAN) bus, ZigBee and Bluetooth. The network layer is capable of handling network and transport connectivity. The service and application support layer aimed to provide a support function for various IIoT applications includes data curation, processing or storage. The application layer consists of IIoT applications. Thereafter, Cisco [54] proposed a seven-layer IIoT reference architecture comprising physical devices and controllers, connectivity, edge or fog computing, data accumulation, data abstraction, application, collaboration and processes layers. The physical devices and controllers layer includes various endpoints that can generate data, be queried and managed. The connectivity layer refers to the communication and connectivity either between devices, local networks or across the networks globally. Transforming network data flows into an appropriate data format for high-level data processing and storage occurred in the edge or fog computing layer. The data accumulation layer is responsible for data storage, whereas the abstraction layer involves aggregating and rendering data and storage to serve the client application. The application layer refers to the IIoT application such as business intelligence and big data analytic applications, sensors control applications and mobile applications. The relationship between the three-layer, four-layer, five-layer and seven-layer IIoT architectures is correlated, and their correlation is further mapped and illustrated in **Figure 1**.

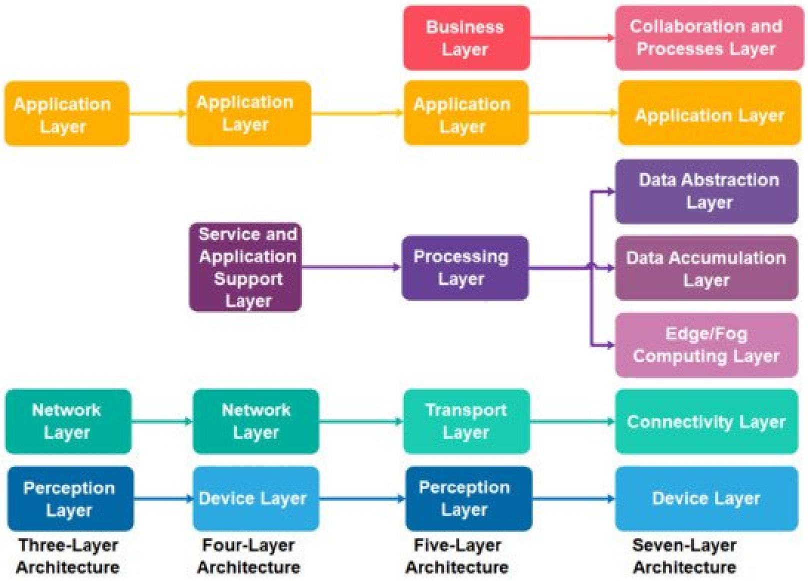

**Figure 1.** The relationship and mapping of three-layer, four-layer, five-layer and seven-layer IIoT architectures.

### 3.2. The Proposed IIoT Security Architecture

This subsection presents the proposed four-layer IIoT security architecture, as illustrated in **Figure 2**. We propose a four-layer IIoT security architecture to solve the shortcomings in current IIoT architectures [15][22][23][24][25][26][27][28][29][30][31][32][33][34][35][36][37][38][39][40][41], which are generic and difficult to address in industrial settings. For example, three-layer IoT architecture fails to satisfy the need for data curation, processing, and storage in IIoT. Subsequently, we classify recent industry IoT technologies and standards into the proposed IoT security architecture for conducting end-to-end security analysis. The security analysis on the device layer focuses on the physical and virtual “things” identification schemes used to connect to IIoT networks. These schemes include EPC, ucode, MAC and IP addresses. On the other hand, security analysis on transport and network layers focuses on IIoT communication technologies and standards, including capillary, backhaul, and backbone networks. The processing layer addresses the end-to-end data protection issues of IIoT data processing platform. Lastly, the application layer addresses the application threats, host-to-host, and client-server application protocol challenges, such as simple object access protocol (SOAP), representational state transfer hypertext transfer protocol (REST HTTP) and data distribution service for real-time systems (DDS).

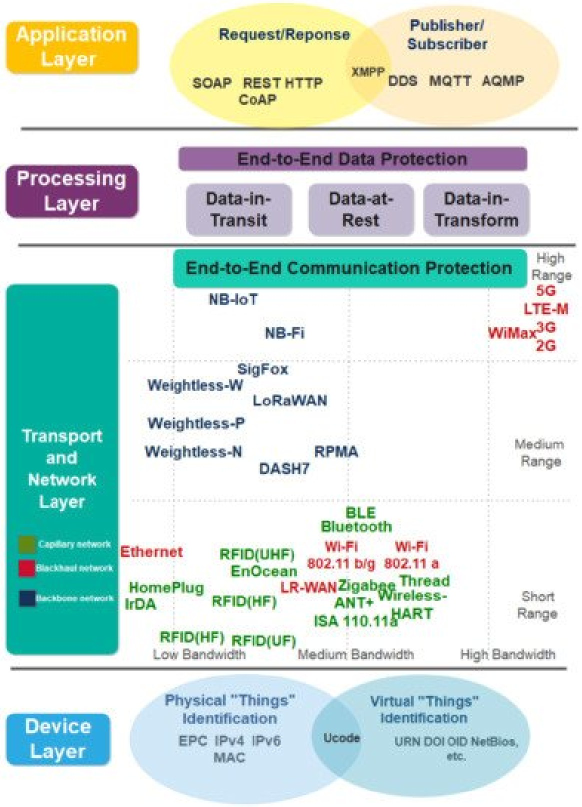

**Figure 2.** The proposed IIoT security architecture.

## References

1. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. Comput. Netw. 2010, 54, 2787–2805.
2. Weber, R.H. Internet of Things–New security and privacy challenges. Comput. Law Secur. Rev. 2010, 26, 23–30.
3. Miorandi, D.; Sicari, S.; De Pellegrini, F.; Chlamtac, I. Internet of things: Vision, applications and research challenges. Ad Hoc Netw. 2012, 10, 1497–1516.
4. Zhao, K.; Ge, L. A Survey on the Internet of Things Security. In Proceedings of the 9th International Conference Computational Intelligence Security-CIS, Emeishan, China, 14–15 December 2013; pp. 663–667.
5. Ziegeldorf, J.H.; Morchon, O.G.; Wehrle, K. Privacy in the Internet of Things: Threats and challenges. Secur. Commun. Netw. 2014, 7, 2728–2742.
6. Jing, Q.; Vasilakos, A.V.; Wan, J.; Lu, J.; Qiu, D. Security of the Internet of Things: Perspectives and Challenges. Wirel. Netw. 2014, 20, 2481–2501.
7. Fremantle, P.; Scott, P. A Security Survey of Middleware for the Internet of Things. PeerJ PrePrints 2015, 3, e1521. Available online: https://peerj.com/preprints/1241.pdf (accessed on 4 October 2021).
8. Granjal, J.; Monteiro, E.J.; Silva, S. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Commun. Surv. Tutor. 2015, 17, 1294–1312.
9. Nguyen, K.T.; Laurent, M.; Oualha, N. Survey on Secure Communication Protocols for the Internet of Things. Ad Hoc Netw. 2015, 32, 17–31.
10. Airehrour, D.; Gutierrez, J.; Ray, S.K. Secure Routing for Internet of Things: A Survey. J. Netw. Comput. Appl. 2016, 66, 198–213.
11. Qin, Y.; Sheng, Q.Z.; Falkner, N.J.G.; Dustdar, S.; Wang, H.; Vasilakos, A.V. When Things Matter: A Survey on Data-Centric Internet of Things. J. Netw. Comput. Appl. 2016, 64, 137–153.
12. Loi, F.; Sivanathan, A.; Hassan, H.G.; Radford, A.; Sivaraman, V. Systematically Evaluating Security and Privacy for Consumer IoT Devices. In Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, New York, NY, USA, 3 November 2017; pp. 1–6.
13. Fernández-Caramés, T.M.; Fraga-Lamas, P. A Review on the use of Blockchain for the Internet of Things. IEEE Access 2018, 6, 32979–33001.
14. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access 2019, 7, 82721–82743.
15. Berkay, C.; Fernandes, E.; Pauley, E.; Tan, G.; McDaniel, P. Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities. ACM Comput. Surv. 2019, 52, 1–30.
16. Tabrizi, F.M.; Pattabiraman, K. Design-Level and Code-Level Security Analysis of IoT Devices. ACM Trans. Embed. Comput. Syst. 2019, 18, 1–25.
17. Amanullah, M.A.; Habeeb, R.A.A.; Nasaruddin, F.H.; Gani, A.; Ahmed, E.; Nainar, A.S.M.; Akim, N.M.; Imran, M. Deep Learning and Big Data Technologies for IoT security. Comput. Commun. 2020, 141, 495–517.
18. Lao, L.; Li, Z.; Hou, S.; Xiao, B. A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling. ACM Comput. Surv. 2020, 53, 1–32.
19. João, B.; Sequeiros, F.; Francisco, T.; Chimuco, M.; Samaila, G.; Freire, M.M.; Pedro Inácio, R.M. Attack and System Modeling Applied to IoT, Cloud, and Mobile Ecosystems: Embedding Security by Design. ACM Comput. Surv. 2020, 53, 1–32.
20. Polychronou, N.-P.; Thevenon, P.-H.; Puys, M.; Beroulle, V. A Comprehensive Survey of Attacks without Physical Access Targeting Hardware Vulnerabilities in IoT/IIoT Devices, and Their Detection Mechanisms. ACM Trans. Des. Autom. Electron. Systems 2021, 27, 1–35.
21. Gaspar, P.D.; Fernandez, C.M.; Soares, V.N.G.J.; Caldeira, J.M.L.P.; Silva, H. Development of Technological Capabilities through the Internet of Things (IoT): Survey of Opportunities and Barriers for IoT Implementation in Portugal's Agro-Industry. Appl. Sci. 2021, 11, 3454.
22. Wu, Y.; Wang, Z.; Ma, Y.; Leung, V.C. Deep reinforcement learning for blockchain in industrial IoT: A survey. Comput. Netw. 2021, 191, 108004.

23. Latif, S.; Idrees, Z.; e Huma, Z.; Ahmad, J. Blockchain technology for the Industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions. Trans. Emerg. Telecommun. Technol. 2021, 191, e4337.

24. Gilchrist, A. IIoT Reference Architecture. In Industry 4.0; Apress: Berkeley, CA, USA, 2016.

25. Ghosh, A.; Mukherjee, A.; Misra, S. SEGA: Secured Edge Gateway Microservices Architecture for IIoT-based Machine Monitoring. IEEE Trans. Ind. Inform. 2021.

26. Lamis, R.D.; Mohamed, T.E.-W.; Mahmoud, M.F. Towards sustainable industry 4.0: A green real-time IIoT multitask scheduling architecture for distributed 3D printing services. J. Manuf. Syst. 2021, 61, 196–209.

27. Chandra, S.R.V.; Kumarswamy, P.; Phridviraj, M.S.B.; Venkatramulu, S.; Subba, R.V. 5G Enabled Industrial Internet of Things (IIoT) Architecture for Smart Manufacturing. Lect. Notes Data Eng. Commun. Technol. 2021, 63, 193–201.

28. International Telecommunication Union. Overview of the Internet of Things. Available online: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items (accessed on 4 October 2021).

29. Ashton, K. That ‘Internet of Things’ Thing. RFiD J. 2009, 22, 97–114. Available online: http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf (accessed on 4 October 2021).

30. Minerva, R.; Biru, A.; Rotondi, D. Towards a definition of the Internet of Things (IoT). IEEE Internet Things 2015, 1–86. Available online: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf (accessed on 4 October 2021).

31. W3C. Web of Things at W3C. Available online: https://www.w3.org/WoT/ (accessed on 4 October 2021).

32. Noura, M.; Atiquzzaman, M.; Gaedke, M. Interoperability in Internet of Things: Taxonomies and Open Challenges. Mob. Netw. Appl. 2019, 24, 796–809.

33. Internet Architecture Board (IAB). Architectural Considerations in Smart Object Networking, RFC 7452. Available online: https://tools.ietf.org/html/rfc7452 (accessed on 4 October 2021).

34. Ning, H.; Wang, Z. Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework? IEEE Commun. Lett. 2011, 15, 461–463.

35. Guinard, D. A Web of Things Application Architecture-Integrating the Real-World into the Web. Ph.D. Thesis, University of Fribourg, Fribourg, Switzerland, 2011. Available online: https://webofthings.org/dom/thesis.pdf (accessed on 4 October 2021).

36. Gómez-Goiri, A.; López-de-Ipiña, D. On the Complementarity of Triple Spaces and the Web of Things. In Proceedings of the Second International Workshop on Web of Things-WoT 11, San Francisco, CA, USA, 12–15 June 2011; pp. 1–6.

37. Vernet, D.; Zaballos, A.; Martin De Pozuelo, R.; Caballero, V. High Performance Web of Things Architecture for the Smart Grid Domain. Int. J. Distrib. Sens. Netw. 2015, 11, 347413.

38. Olivier, F.; Carlos, G.; Florent, N. New Security Architecture for IoT Network. Procedia Comput. Sci. 2015, 52, 1028–1033.

39. Qin, Z.; Denker, G.; Giannelli, C.; Bellavista, P.; Venkatasubramanian, N. A Software Defined Networking Architecture for the Internet-of-Things. In Proceedings of the IEEE Network Operator Management Symposium (NOMS), Krakow, Poland, 5–9 May 2014; pp. 1–9.

40. Bauer, M.; Boussard, M.; Bui, N.; Carrez, F. Project Deliverable D1.5–Final Architectural Reference Model for IoT, IoT-A. Available online: https://cordis.europa.eu/project/id/257521 (accessed on 4 October 2021).

41. iCore? D2.5 Final Architecture Reference Model, iCore. Available online: https://cordis.europa.eu/docs/projects/cnect/8/287708/080/deliverables/001-20141031finalarchitectureAres20143821100.pdf (accessed on 4 October 2021).

42. SENSEI. Available online: http://www.sensei-project.eu/ (accessed on 4 October 2021).

43. D1.2.2 Final COMPOSE Architecture Document, FP7-317862-COMPOSE. 2018. Available online: https://cordis.europa.eu/project/id/317862 (accessed on 4 October 2021).

44. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Gener. Comput. Syst. 2013, 29, 1645–1660.

45. Farris, I.; Militano, L.; Nitti, M.; Atzori, L.; Iera, A. MIFaaS: A Mobile-IoT-Federation-as-a-Service model for dynamic cooperation of IoT Cloud Providers. Future Gener. Comput. Syst. 2016, 70, 126–137.

46. Conti, M.; Kaliyar, P.; Lal, C. CENSOR: Cloud-enabled secure IoT architecture over SDN paradigm. Concurr. Comput. Pract. Exp. 2018, 31, e4978.

47. Park, S.; Park, S. A Cloud-based Middleware for Self-Adaptive IoT-Collaboration Services. Sensors 2019, 19, 4559.

48. Devadas, T.J.; Subramanian, R.R. Paradigms for Intelligent IOT Architecture. In Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm; Springer: Berlin/Heidelberg, Germany, 2020; Volume 174, pp. 67–100.
49. Memon, R.A.; Li, J.P.; Nazeer, M.I.; Khan, A.N.; Ahmed, J. DualFog-IoT: Additional Fog Layer for Solving Blockchain Integration Problem in Internet of Things. IEEE Access 2019, 7, 169073–169093.
50. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Zhang, Q.; Choo, K.-K.R. An Energy-efficient SDN Controller Architecture for IoT Networks with Blockchain-based Security. IEEE Trans. Serv. Comput. 2020, 13, 625–638.
51. Medhane, D.V.; Sangaiah, A.K.; Hossain, M.S.; Muhammad, G.; Wang, J. Blockchain-enabled Distributed Security Framework for Next Generation IoT: An Edge-Cloud and Software Defined Network Integrated Approach. IEEE Internet Things J. 2020, 7, 6143–6149.
52. Telecommunication Standardization Sector ITU-T Y.2002 Overview of Ubiquitous Networking and of Its Support in NGN. Int. Telecommun. Union 2009. Available online: https://www.itu.int/rec/T-REC-Y.2002-200910-I/en (accessed on 4 October 2021).
53. Wu, M.; Lu, T.J.; Ling, F.Y.; Sun, J.; Du, H.Y. Research on the Architecture of Internet of Things. In Proceedings of the 3rd International Conference Advanced Computer Theory Engineering 2010, Chengdu, China, 20–22 August 2010; pp. 484–487.
54. Candanedoa, I.-S.; Alonso, R.S.; Corchado, J.M.; González, S.R.; Vara, R.C. A review of edge computing reference architectures and a new global edge proposal. Future Gener. Comput. Syst. 2019, 99, 278–294.