A pattern for a Secure Cloud-Based IoT Architecture

EDUARDO B. FERNANDEZ, Florida Atlantic University

IoT systems are very complex systems with a extensive attack surface which makes them susceptible to a large variety of threats. Their high complexity and large number of vulnerabilities require some global control for the coordination and management of their defenses. To provide this control, handle large amounts of data, and decrease latency, IoT architectures, in addition to things, often include cloud and fog systems. We present here a pattern that describes this architecture, indicating its threats and corresponding defenses. The pattern defines security protection for data assets and for the communication channels in order to neutralize the IoT system threats and reduce the complexity of managing security. The defenses include authentication, authorization, security logger/auditor, secure channel, and firewall/Intrusion Detection System (IDS). This is an addition to a set of patterns focusing on the security of IoT ecosystems, being built by our group.

Categories and Subject Descriptors: D.2.11 **[Software Engineering]** Software Architectures–Patterns;

General Terms: Design

Additional Key Words and Phrases: Security patterns, secure software, software architecture, IoT, network segmentation

ACM Reference Format:

Fernandez, E.B., "A pattern for a Secure Cloud-Based IoT Architecture". Procs. of the 27th Conf. on Pattern Langs. of Progs. (PLoP'20), October 2020, 9 pages.

1. INTRODUCTION.

Security is a very important issue for any type of systems and in particular for IoT systems where a large variety of possibly suspicious devices may need to be integrated as part of applications. IoT systems are very complex systems with a large attack surface and are susceptible to a large variety of threats. This complexity and large number of vulnerabilities require some global control for the coordination and management of their defenses. To provide this control and decrease latency, IoT architectures, in addition to things, often include cloud and fog systems. Clouds are increasingly used to program, control, and manage IoT systems (Dizdarevic et al. 2019, Gubbi et al. 2013, Truong and Dustdar 2015). Fog Computing is a virtualized platform that stands between cloud computing systems and Internet devices (things), providing to them computation, storage, and networking services and allowing a cloud to control and communicate with the fog and the devices to perform some functions with them, such as controlling traffic lights, collect temperature readings in a city, and many others. We present here a pattern for a secure IoT architecture. Fig. 1 shows a typical IoT architecture where devices or things are managed by fogs and clouds.

The protection of this architecture is performed by a combination of security patterns. As shown in Figure 2, the IoT ecosystem includes patterns for the secure IoT architecture, secure cloud, secure fog, secure thing, secure actuator, and secure sensor. We are building all these patterns. The intents of these patterns are:

Secure Cloud-Based IoT Architecture (this pattern): Define security protection for data assets and for the communication channels in order to neutralize the system threats and reduce the complexity of managing security. The defenses include authentication, authorization, security logger/auditor, and secure channel.

Secure Cloud. A Cloud Security Reference Architecture (SRA) describes its threats and corresponding defenses (Fernandez et al. 2016). Due to the complexity and variety of clouds, a reference architecture is more useful that just a composite pattern.

Author's address: Eduardo B. Fernandez (corresponding author), Dept. of Computer and Electrical Eng. and Computer Science, Florida Atlantic
University, 777 Glades Rd., Boca Raton, FL33431, USA; email: fernande@fau.edu

Secure Fog. Fog Computing is a virtualized platform that stands between cloud computing systems and Internet devices, providing to these computational, storage, and networking services and allowing a cloud to control and communicate with these devices and to the devices to send data to the fog or the cloud (Syed et al. 2016).

Secure Thing. An entity with sensors and actuators where the data and channels are secured (pattern in progress). Common things are devices such as phones, but they can be drones, smart lights, smart appliances, and others

Secure Actuator. A component of a system that can control a physical system (pattern in progress).

Secure Sensor Node. Describe the architecture of a unit intended to sense, store, and communicate local information about a physical environment. For those purposes the node architecture includes sensors, memory, and communication channels and their data and communication channels are protected (Orellana et al., 2020).

Institution in Fig. 1 represents the fact that some devices (things) may be controlled or owned by some entity which may apply security constraints and/or manage the devices.

Our audience includes IoT application designers, cloud/fog developers that may need to interact with IoT systems, security researchers and students.

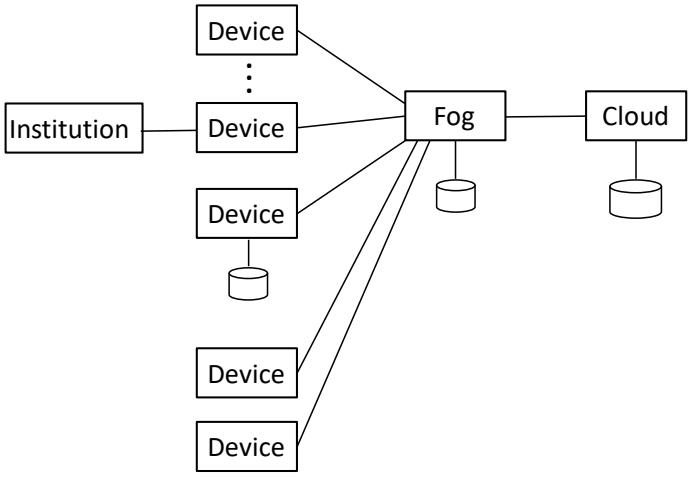

Fig. 1. A typical IoT architecture

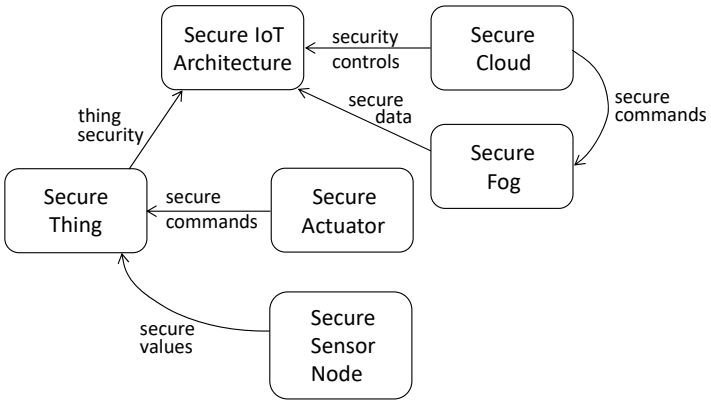

Fig. 2. Pattern diagram of IoT secure architecture ecosystem.

2. SECURE CLOUD-BASED IOT ARCHITECTURE

2.1 Intent

Define security protection for data assets and for the communication channels in order to neutralize the IoT system
threats and reduce the complexity of managing security. The defenses include authentication, authorization, security logger/auditor, secure channel, and firewall/Intrusion Detection System (IDS).

2.2 Context

Some applications, e.g. traffic light control, require performing a variety of functions with existing devices. Some of these applications may be stand alone or may be part of a larger cyber-physical system, e.g. a traffic light control may be part of the infrastructure of a smart city.

2.3 Problem

We have a network with a large number of IoT devices from different origins and owners, many of which may have only basic or no security defenses. This situation lets hackers try a large variety of attacks. How can we protect the data handled by these devices and the control of the devices themselves?

The solution of this problem is constrained by the following forces:

- *Quantity of things*. Most IoT applications involve a large amount of things, e.g. city traffic light control systems (Ghena et al., 2014). This results in a large number of possibly different things with different access constraints, which makes their security management very complex.
- *Diversity of things*. Some applications use things coming from different vendors and possibly with different owners, who may still have some control of the devices.
- *Vulnerability of things*. Most things are rather inexpensive and have low computational power. This means that they do not have elaborated defenses; for example, if they use cryptography, it is lightweight versions.

2.4 Threats.

We only consider here threats affecting things and their interactions with actuators, sensors, fogs, and clouds. For threats that affect fogs and clouds see the corresponding patterns or RAs.

- *Distributed Denial of Service (*DDoS) (Syed and Fernandez 2018). An attacker intends to make a target unavailable by flooding its resources with a large volume of traffic using IoT devices (Availability attack). Many IoT devices can be commanded to send continuously messages to the target after converting them into bots.

- *Unauthorized access to the data in a thing*. A thing may have several types of data storage that can be accessed (read or modified) by hackers (confidentiality or integrity attack).

- *Unauthorized data access in another thing or component*. The attacker, after compromising a thing, intends to access data in another thing or in some external server (confidentiality or integrity attack).

- *Wrong command to actuator*. The command may produce a physical action that causes damage to people or physical assets (disruption attack). As example, (Ronen and Shamir 2016) showed that commands can be used as covert channels to leak sensitive information and to trigger seizures in photosensitive people.

- *Unauthorized modification of sensor data*. False information is sent from the sensor to the thing producing confusion on its processing (disruption attack).

- *Authorization inconsistencies between levels.* Clouds, Fogs, and things may have authorization rules controlling their data. These rules may have inconsistencias that could allow a hacker to have unauthorized access to data.

2.5 Solution

Define security protection for the IoT data assets and for the communication channels in a hierarchy of layers in order to neutralize the system threats and reduce the complexity of managing security in the IoT architecture.

2.5.1 *Structure*

An application can be executed from an institution or a cloud and can use IoT devices in all or part of its functions. Fig. 3 shows a UML class diagram of a typical IoT architecture. Owner may be a cloud service provider or an institution. Thing is a device or any IoT component. Thing Type groups similar things. Things may be connected to other things. Each layer in this architecture may have its own data.

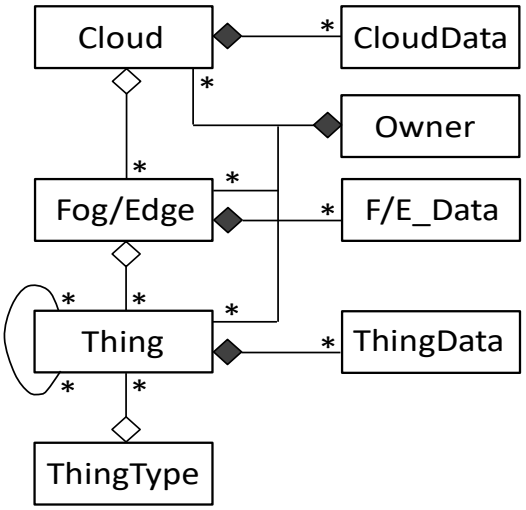

Fig. 3. Class diagram of an IoT architecture.

2.5.2 *Dynamics*

To analyze security in an architecture we need to observe how attacks would happen and show how they could be stopped with the added security mechanisms. If all the possible attacks can be neutralized, we consider the system secure (Villagran et al. 2020).

A sequence diagram for DDoS attacks is shown in (Syed and Fernandez 2018). In 2.6 we show possible defenses. Another example is shown in (Romero and Fernandez, 2020). This is an example of the *Wrong command to actuator* threat.

2.6 Countermeasures

Figure 4 shows the addition of security defenses to control the identified threats (shown in light blue). These defenses include:

DDoS (See (Syed et al. 2018) for a complete list of possible defenses):

- IoT devices can be given limited communication capabilities to prevent direct interaction with devices other than intended collaborators over the internet (see (L. Reinfurt et al. 2017)).
- IoT devices need to be patched or fixed for known vulnerabilities as soon as these security updates become available to prevent their exploitation.
- Firewalls and IDS in Fogs can be used at this level to filter ingress and egress traffic to/from IoT devices.
- Bot/malicious IoT devices can be isolated from the rest of the network upon detection, possibly using segmentation.

Unauthorized data access. Add Authenticator, Authorizer, and Security Logger/Auditor to the thing (Fernandez 2013).

Unauthorized data access in another thing or component. Isolation can be obtained by physical separation and by controlled interfaces (Brambilla et al. 2017).

Wrong command to actuator. Actuators may have controlled interfaces (Brambilla et al. 2017). Other defenses are found in in (Romero and Fernandez, 2020).

Unauthorized modification of sensor data. Add Secure Channel pattern (Fernandez 2013).

Authorization inconsistencies between levels. A possible solution is discussed in (C. Wood et al. 1979)

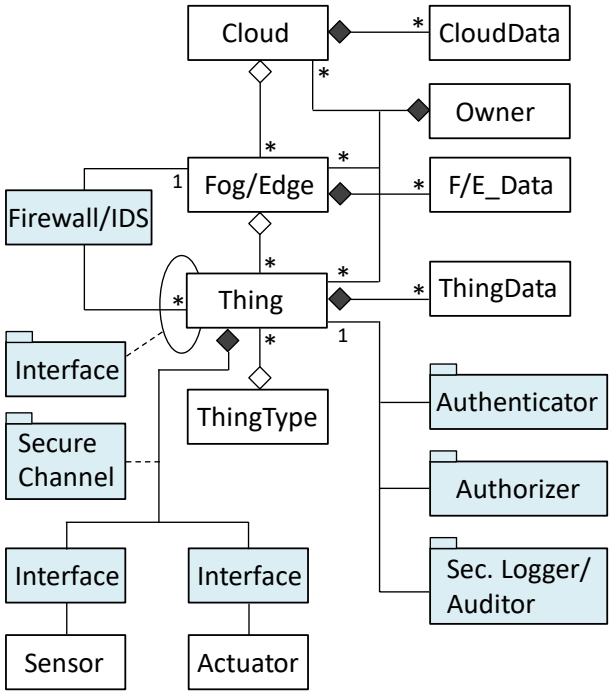

Fig. 4. A secure IoT architecture

2.7 Implementation

IoT architectures can be centralized, collaborative, connected intranet, and distributed (Roman et al., 2013). We assumed a distributed architecture in our class model, but the other configurations can be easily derived. However, they may have different security properties. The specific networks used to connect the things also have an effect on the security properties of the system.

A reference architecture (RA) from Microsoft (Microsoft 2018) shows a typical implementation of their RA which incorporates a cloud gateway, two types of storage, machine learning, and user interfaces (Figure 5). The user interfaces can be used to restrict access (authentication and authorization), the gateway can support secure data communications using encryption, digital signatures, and TLS. Protection against physical tampering can be obtained using secure bootloader and secure software loading supported by a TPM. Edge devices are optional.

An architecture for IIoT is shown in Figure 6 (Wikipedia 2020). This architecture consists of several manufacturing lines, some fixed, some wireless, has provisions for real-time processing, and uses gateways to control access to each line. It does not use fogs, but it would easy to add them.

In order to improve management and control at the cost of higher complexity, it is also possible to have a hierarchy of fogs (Puliafito et al. 2019).

The networks connecting things control access using Gateways, which can apply authentication or secure protocols like TLS. The choice of network protocols can have a big effect on the complexity of the system and thus on security (Dizdareviz et al. 2019).

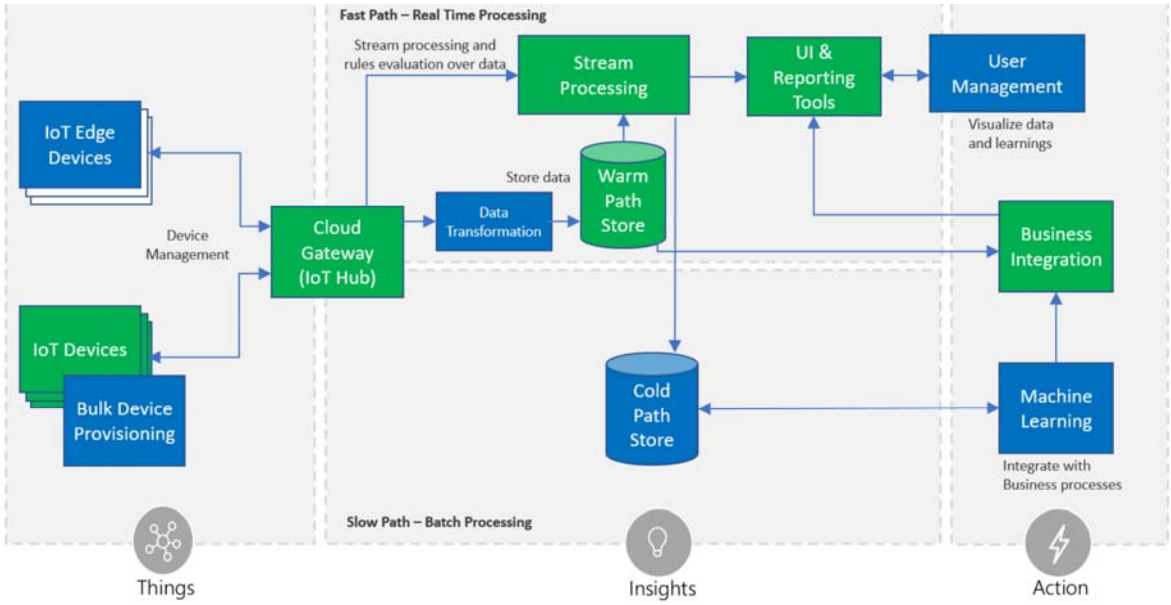

Fig.5. Azure IoT reference architecture (from (Microsoft 2018))

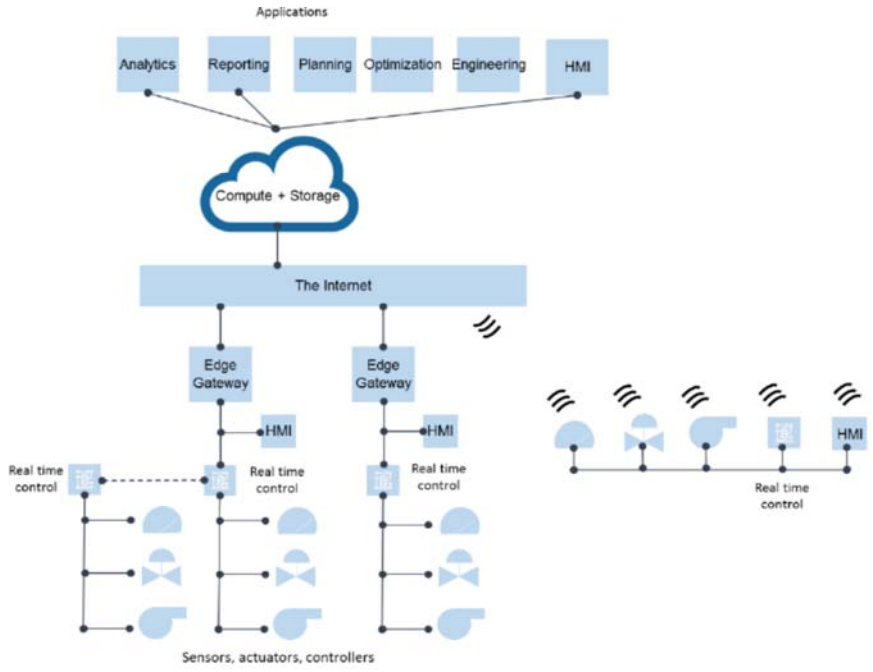

Fig. 6 An architecture for manufacturing systems (from (Wikipedia 2020

2.8. Known uses

- (Thramboulidis et al. 2018) proposed an IoT architecture for manufacturing using microservices. This architecture uses a cloud, fog systems, and microservices running on IoT devices.
- (Puliafito et al. 2019) consider several varieties of this architecture.
- (Leander et al. 2019) describes manufacturing architectures that also include SCADA systems in the hierarchy.
- (Ray 2018) shows several IoT architectures used in different types of applications.

2.9. Consequences

This pattern provides the following advantages:

- *Quantity of things*. It is possible to identify individual things using identity patterns (Delessy et al., 2008). We also have ways to group authorization rules including rule inheritance and aggregation (Fernandez et al. 1975).
- *Diversity of things*. We can apply abstraction to the thing descriptions, focusing on their essential aspects. Abstraction can be used to define conceptual defenses based on abstract security patterns (Fernandez 2013).
- *Vulnerability of things*. For those things with poor security defenses we can define wrappings that apply an extra layer of control.
- *Threats*. As shown in the solution section, all the threats have been properly handled.

Liabilities include:

- Overhead. Security always implies some overhead, adding these defenses will have an effect on performance.
- Complexity. The addition of several defense mechanisms will increase the complexity of the system.
- Cost. Most IoT devices are low cost. Adding elaborate security defenses will increase the cost of the system.

2.10. Related patterns

- Fog Computing (Syed et al. 2016) – describe the fog computing platform that can be used to support IoT ecosystems.
- Identity patterns (Delessy et al. 2008, Fernandez 2013)—define a structure to identify components in distributed systems. They include the Identity Provider, Identity Federation, and Circle of Trust.
- Secure Thing—Under development.
- Secure Actuator—Under development.
- Secure Sensor Node (Orellana et al. 2020)-- a pattern whose purpose is to obtain, store and subsequently transmit data securely from a physical environment, to other nodes or Information Systems.
- Security interface (Brambilla et al., 2017). Any of the components of this architecture may have its own security interface that can be used to enforce security constraints.
- Security Cloud Reference Architecture (Fernandez et al. 2016)—An abstract cloud architecture showing defenses to typical threats.
- Entity-Component-Attribute on Linked Data Platform (Washizaki et al.2020) -- Support the design of changeable and maintainable software components for large-scale IoT applications.
- Trusted Platform Module (TPM) (operations (Muñoz and Fernandez 2020) provides assured software execution by verifying that the hardware and software are legitimate and can be trusted before execution takes place. A chain of trust and an integrated set of cryptographic keys are fundamental for that purpose. It may also (or instead) be intended to store secret keys and perform encryption or decryption on request
- An IoT architecture that includes several models that could become patterns is presented in (Patel and Cassou 2015).

3. CONCLUSIONS

We need a variety of patterns to facilitate the secure design the complex architectures involved in IoT-based systems. We have initiated a project to build a set of patterns for IoT design. These already include (E.B.Fernandez et al. 2019 and 2020). This pattern and its companions join this set. Another and complementary direction includes hardware-based devices that can be used to attest the authenticity of platforms based on cryptographic operations (Muñoz and Fernandez 2020).

Note that the class diagram of the patterns indicates components and defenses that may not be present in specific systems; the pattern must be considered as a paradigm, not as a system description.

ACKNOWLEDGMENTS

We thank our shepherd Prof. Antonio Muñoz for his useful comments that improved the quality of this work. The participants in the virtual PLoP 2020, Denys Poltorak, Cristian Orellana, and Kyle Brown, provided useful comments.

REFERENCES

M. Brambilla, et al., "Model-driven development of user interfaces for iot systems via domain-specific components and patterns," J. of Internet Services and Applications, 8(1), 2017

F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad, M. Stal. Pattern-Oriented Software Architecture: A System of Patterns, Vol. 1. J. Wiley, 1996.

Mihaela Cardei, E.B.Fernandez, Anupama Sahu, and Ionut Cardei, "A pattern for Wireless System Architectures", Procs. of Asian PLoP 2011.

N. Delessy, E.B.Fernandez, and M.M. Larrondo-Petrie, "A pattern language for identity management", Procs. of the 2nd IEEE Int. Multiconference on Computing in the Global Information Technology (ICCGI 2007), March 4-9, Guadeloupe, French Caribbean. http://www.computer.org/portal/web/csdl/doi/10.1109/ICCGI.2007.5

J. Dizdarevic, F. Carpio, A. Jukan, "A survey of communication protocols for Internet of Things and related challenges of fog and cloud computing integration", ACM Comp. Surveys, vol. 51, No 6, Article 116, January 2019.

E. B. Fernandez, R. C. Summers and T. Lang, ``Definition and Evaluation of Access Rules in Data Management Systems," *Proceedings 1st International Conference on Very Large Databases*, Boston, 1975, 268-285.

E.B.Fernandez, J. Ballesteros, A. C. Desouza-Doucet, and M.M. Larrondo-Petrie, "Security Patterns for Physical Access Control Systems", in S. Barker and G.J. Ahn (Eds.), Data and Applications Security XXI, LNCS 4602, 259-274, Springer 2007.

E.B.Fernandez, "Security patterns in practice: Building secure architectures using software patterns", Wiley Series on Software Design Patterns, 2013.

E.B.Fernandez, Raul Monge, and Keiko Hashizume, "Building a security reference architecture for cloud systems", *Requirements Engineering*., June 2016, Volume 21, Issue 2, 225-249. Doi: 10.1007/s00766-014-0218-7

E.B.Fernandez, N. Yoshioka, H. Washizaki, M. Syed, "Modeling and security in cloud ecosystems", Future Internet 2016, 8(2), 13; doi:10.3390/fi8020013, (Special Issue Security in Cloud Computing and Big Data

E.B.Fernandez, N. Yoshioka, H. Washizaki, "Abstract and IoT security segmentation patterns", Procs. of Asian PLoP 2019

E.B.Fernandez, N. Yoshioka, H. Washizaki, "Secure distributed Publish/Subscribe (P/S) pattern for IoT", Procs. of AsianPLoP 2020.

Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman, "Green Lights Forever: Analyzing the Security of Traffic Infrastructure", WOOT'14: Proceedings of the 8th USENIX conference on Offensive Technologies, August 2014

J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions", Future Generation Computer Systems, 29, 2013, 1645-1660.

Björn Leander, Aida Causevic, Hans Hansson, Applicability of the IEC 62443 standard in Industry 4.0 / IIoT. ARES 2019, 101:1-101:8

Microsoft. "Microsoft Azure IoT reference architecture", Version 2.1, Sept. 26, 2018, https://aka.ms/iotrefarchitecture

A. Muñoz and E.B.Fernandez, "TPM, a pattern for an architecture for trusted computing", PLoP 2020.

N.Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N.Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations", IEEE Comm. Surveys & Tutorials, April 2019.

C. Pahl, N. El Ioni, S. Helmer, B. Lee, "An architecture pattern for trusted orchestration in IoT edge clouds", CLOSER 2018: 221-232.

P. Patel, D. Cassou, "Enabling high-level application development for the Internet of Things", J. of Systs. and Software, 103, 2015, 62-84.

Carlo Puliafito, Enzo Mingozzi, Francesco Longo, Antonio Puliafito, and Omer Rana. 2019. "Fog Computing for the Internet of Things: A Survey". ACM Trans. Internet Technol. 19, 2, Article 18 (April 2019), https://doi.org/10.1145/3301443

P.P. Ray, "A survey on Internet of Things architectures", J. of King Saud University—Comp. and Information Systs., vol. 30, 2018, 291-319

L. Reinfurt, U. Breitenbucher, M.Falkenthal, P.Fremantle, F. Leymann, "Internet of Things security patterns", Procs. of PLoP'17, Vancouver, CA, Oct. 2017, https://dl.acm.org/citation.cfm?id=3290281.3290305

R. Roman, J. Zhou, J. Lopez. “On the features and challenges of security and privacy in distributed internet of things”. Computer Networks 2013;57(10):2266–79.
E. Ronen, A. Shamir, “Extended functionality attacks in IoT devices: The case of smart lights”, 2016 IEEE European Symp. on Security and Privacy, 3-12.
Virginia M. Romero, E. B. Fernandez, "Misuse Patterns Derived from Threats that Take Control of Radio Frequency Remote Controllers of Container Terminal Cranes", Procs. of AsianPLoP 2020.
Anupama Sahu, E.B. Fernandez, Mihaela Cardei, M. VanHilst, "A pattern for a sensor node", Procs. 17th Conf. on Pattern Languages of Programs, PLoP 2010.
M.G.Samaila, J.B. Siqueiros, M.M.Freire, P.R.M.Inacio, “Security threats and possible countermeasures in IoT”, Procs. ARES 2018
Madiha H. Syed, E.B.Fernandez, M.Ilyas, “A pattern for fog computing”, Procs. of Pattern Languages of Programming (VikingPLoP 2016), 7th-10th April 2016, Leerdam, Netherlands, ACM New York, NY, USA doi>10.1145/3022636.3022649
Madiha H. Syed, E.B. Fernandez, “A misuse Pattern for DDoS in the IoT”, EuroPLoP’17, Irsee, Germany, July 2018.
K. Thramboulidis, D.C. Vachtsevanou, A. Solanos, “Cyber-physical microservices: An IoT-based framework for manufacturing systems”. ICPS 2018*: 232-239*
H.L. Truong, S. Dustdar, “Principles for engineering IoT cloud systems”, IEEE Cloud Comp., 2(2), March-April 2015, 68-76.
Olga Villagran-Velasco, E.B.Fernandez, Jorge Ortega-Arjona, “Refining the evaluation of the degree of security of a system built using security patterns”, Procs. 15th International Conference on Availability, Reliability and Security (ARES 2020), Dublin, Ireland, Sept. 2020.
H. Washizaki, N. Yoshioka, A. Hazeyama, T. Kato, H. Kaiya, S. Ogata, T. Okubo and E. B. Fernandez, “ Landscape of IoT Patterns”, accepted for the IEEE Internet of Things Journal.
Wikipedia, “Industrial Internet of Things”, 2020, https://en.wikipedia.org/wiki/Industrial_internet_of_things
C. Wood, R. Summers, and E. B. Fernandez, ``Authorization in Multilevel Database Models,'' Information Systems, Vol 4, pp. 155-161, 1979.
Z.-K.Zhang, M. C.Y.Cho, S. Shieh, “Emerging security threats and countermeasures in IoT”, ASIA CCS’15, ACM, April 2015, Singapore.