# Towards a Visual Grammar for IoT Systems Representation and their Cybersecurity Requirements

Alain Gómez-Cabrera
Instituto Politécnico Nacional
Centro de Investigación en Computación
Mexico City, Mexico
alngoca@gmail.com

Ponciano J. Escamilla-Ambrosio
Instituto Politécnico Nacional
Centro de Investigación en Computación
Mexico City, Mexico
pescamilla@cic.ipn.mx

Abraham Rodríguez-Mota
Instituto Politécnico Nacional
Centro de Investigación en Computación
Mexico City, Mexico
arodrigm@cic.ipn.mx

Jassim Happa
Information Security Group
Royal Holloway, University of London
London, UK
jassim.happa@rhul.ac.uk

***Abstract*— In this paper we present progress towards visual iconography (elements) and a grammar for Internet of Things (IoT) system representations and their cybersecurity requirements. Our visual representation of IoT systems aims to facilitate the identification of the IoT attack surface and the vulnerabilities that an attacker may exploit. The paper first outlines the basic visual elements and the associated grammar, which are then applied to a series of smart home IoT use cases to demonstrate how these can be used to represent these networks and their cybersecurity requirements in a visual and intuitive way. The motivation behind this work is to improve our ability to reason about IoT attack surfaces towards improving our defense capabilities for those systems.**

***Keywords*— *Internet of things, Cybersecurity, Visual Grammar, Cyber-Physical Systems, Attack Surface.***

## I. INTRODUCTION

The IEEE defines the Internet of Things (IoT) as "*A network of elements each integrated with sensors, which are connected to the Internet*" [1]. Today, everyday devices can communicate with the Internet creating large and complex networks. Current IoT systems use a wide variety of communications technologies and protocols. Some of the most common communications technologies used in the IoT include RFID, Bluetooth, ZigBee, among many others.

The IoT domain is particularly vulnerable to attacks due to the heterogeneous nature of IoT systems as their threat landscape remains poorly understood. The outcome of unauthorized communication between IoT devices may result in unpredictable harms as manufacturers may not appreciate how the variety of IoT sensors may integrate in a vast heterogeneous environment. The vulnerabilities of an IoT system are related to several aspects such as the characteristics of the devices and the communications protocols involved.

The task of identifying vulnerabilities in systems typically gets easier as complexity increases. In other words, the attack surface of an IoT system grows when we add more elements to it, as these can be an access point for an attack or an intrusion. If we consider the vulnerabilities of each individual component of an IoT system, for each component added to the system we are adding additional vulnerabilities.

978-1-7281-8715-0/20/$31.00 ©2020 IEEE

The National Institute of Standards and Technology (NIST) provides a brief description of what an IoT system is and classifies it as a Cyber-Physical System (CPS) [2]. The physical domain of the IoT adds a new set of security concerns. Physical interactions between things and the environment are critical because they can create additional attack vectors that are difficult to specify, harden and detect.

Mitigation of IoT vulnerabilities remains challenging. On the one hand, the countermeasures to mitigate these types of vulnerabilities can produce an increment in the cost of IoT hardware due to the additional implementation of physical security controls. This undesirable consequence may lead to stakeholders not implementing the appropriate security controls in order to offer a more competitive price of their products to the market. Hardware limitations may also make it infeasible to implement the required controls due to device constrains such as computational power, memory and other resources.

Hence, achieving security goals such as availability, confidentiality and integrity in an IoT system is a complex issue that requires a deep understanding of the system's environment and behaviour. We believe a visual representation would facilitate the analysis of vulnerabilities within an IoT system, making it possible to implement countermeasures more easily and quickly and will help to eliminate or mitigate those vulnerabilities. To achieve this, visual elements are designed for each element in an IoT system and a visual grammar specifies the interactions between them.

The rest of this paper is organized as follows: Section 2 presents related works on representing IoT systems. Section 3 presents the proposed visual elements with their grammar and the strategies used to define them. In section 4, examples of smart home systems are described and then represented with the proposed visual elements and grammar. Finally, Section 5 concludes this work.

## II. RELATED WORKS

Existing systems modeling tools have been adapted as extensions or modules to represent IoT systems. The most common adaptations are based on the Unified Modeling Language (UML) and the Systems Modeling Language (SysML). Some of the disadvantages of using UML and its

extensions include: 1) the amount of advanced knowledge about UML expressions required, and 2) many different diagrams needed to represent the structure and functionality of a system. In turn, these issues can make the system difficult to understand for non-technical users.

An IoT specific domain modeling language based on UML was proposed by Eterovic et al. [3]. This proposal represents devices with labeled rectangles and each device contains one or more elements which represent sensors, actuators or other components and the communication between the elements is carried out through "provided" or "required" interfaces. Circle and semicircle notations are adopted to represent the interfaces of the elements in a friendlier way instead of the traditional UML approach. As the authors mentioned, there is a dilemma between having a powerful tool for modeling IoT systems and having a tool simple enough to be used by a non-expert UML developer. They also discuss the lack of a "de facto" IoT language despite recent efforts in the field.

Robles-Ramírez et al. [4] provided an extension of UML and SysML to evaluate IoT systems security. This extension, called IoTsecM, focuses on considering the security requirements within an IoT system within the design stage. The proposal encapsulates and summarizes the security requirements in a nomenclature and defines a UML class diagram for each cybersecurity requirement.

Another proposal is ASTo, presented by Mavropoulos [5]. ASTo is a software tool that allows the visualization of problems related to the security of the IoT system. ASTo uses the modeling language constructs of the APPARATUS framework [6]. This framework defines two meta models to describe IoT systems: the meta model of the design phase and the implementation phase. Security analysis is facilitated with the use of visualization tools.

As described previously, current approaches to solve the problem of representing an IoT system do not visually consider security aspects. Although there are extensions of modeling methodologies, such as IoTsecM, which include security aspects, the disadvantages of having a model adaptation versus a representation specifically designed to include such considerations are clear: greater simplicity in the diagram, adequate representation elements for the components, unambiguous symbology, etc.

Crypto-protocol analysis literature often uses message sequence charts to illustrate attacker behavior necessary to compromise a protocol [7] but typically only identify where the protocols can be abused, rarely detailing the human-level harms of misuse. Attack graphs and trees [8] are also used to illustrate how the attacker can laterally move on a network, or the capabilities they need to compromise digital assets. We think such approaches struggle to be applied meaningfully outside academia for two key reasons: 1) formal methods are only as good as the assumptions they make, and 2) deploying formal methods can be cumbersome in real-world settings, simply because they require a high-degree of mathematical literacy, and arguably are therefore difficult to adopt by security practitioners.

## III. Design of Visual Elements

### A. Classification of IoT components

As a starting point for this representation, a classification scheme for the components of an IoT system is adopted. For this classification of devices in an IoT ecosystem, the following classes are considered in this paper:

- *Device*. An object that belongs to the ecosystem of the IoT system but does not have the capability to be connected directly to the Internet without an intermediary such as a local data collection device or other IoT device. In other words, it does not have a transceiver that provides a mechanism to communicate directly with the Internet or with an IoT gateway.
- *IoT device*. This group covers the collection of smart devices with a transceiver and which has the ability to exchange data with the cloud through an IoT gateway.
- *Sensor*. In Bauer et al. [9], a sensor is defined as: "*A device that provides information, knowledge, or data about the physical entity it monitors. Sensors can be attached or embedded in the physical structure of the physical entity or be placed in the environment and indirectly monitor physical entities*".
- *Actuator*. A device that performs actions on the environment to obtain a desirable result. In the same way as sensors, actuators can be denoted as IoT devices or devices.
- *Processing unit*. The main task of this type of device is to process the data obtained from the sensors for decision-making or to send data to the cloud for analysis or further processing.
- *Gateway*. In an IoT environment, different technologies co-exist in each layer of the IoT architecture. A device whose job is to translate the packets received from one IoT communications technology to another IoT communications technology is identified as an IoT gateway. Examples of IoT technologies managed by an IoT gateway are Zigbee, LoRa, Bluetooth, 6LowPAN, Wi-Fi, etc.
- *Networking device*. This category includes Internet network hardware devices such as routers, switches, hubs, bridges and repeaters that are required for IoT systems to establish communication with the cloud.

### B. Visual elements

According to Kress and Leeuwen [10], to define a symbol that represents a real-world object, we must choose the most critical property of the object and then select the most appropriate form for its representation. Because of this, it is essential to define the attributes and properties of IoT components and select the one that is characteristic to represent each component. Nakamura and Zeng-Treitler [11] identify several strategies for the design of visual elements: visual similarity, semantic association and arbitrary convention. This proposal starts from developing these strategies to define each

visual element of representation for IoT devices and how they interact.

To design the visual elements of IoT systems, we used a combination of the aforementioned design strategies. The type of device is associated with a geometric pattern that defines the outline of the visual element as shown in Table I. The association between types of components and visual elements makes possible to see the function and role of a component in an IoT system more clearly and improves the communication function of its representation. A more detailed representation of the functionality of devices is provided with the addition of a specific geometric contour for each type. These visual elements are presented in Table II and allow to specify some functions of the devices.

Finally, to distinguish between devices of the same class, an icon is placed within the geometric figure defined by the contour, as shown in Table III for the sensor class, and in Table IV for the actuator class. These icons were selected according to the semantic association metaphor strategy. For example, to represent the idea of moisture, a drop of water is proposed as a visual metaphor. In Table V, the icons are defined for common devices in the IoT environment.

We consider two specific IoT cybersecurity requirements: tamper protection and privacy through encryption. Tamper protection is denoted with a square of stripes on the contour of the visual element. If a visual element has this scratched frame, it represents that such element is provided with a physical mechanism to prevent manipulation.

A lock icon indicates the encryption functionality. If a device encrypts messages sent to another device, then the padlock icon with an arrow pointing up is placed in the corner just below the transceiver icon to indicate that the message leaves the device with its content encrypted. Similarly, if the receiving device of the communication channel performs the decryption function, then a padlock icon with an arrow pointing down below the transceiver icon is placed to indicate this. Table VI summarizes these functionalities.

TABLE I. GEOMETRIC CONTOUR PATTERNS OF IOT DEVICES.

| Device | Contour pattern |
|---|---|
| Sensor or Actuator | Circle |
| Smart Sensor or Actuator | Square |
| Processing unit | Square |
| IoT Gateway | Octagon |
| Networking device | Diamond |

TABLE II. VISUAL ELEMENTS FOR FUNCTIONALITY OF IOT DEVICES.

| Functionality | Visual element |
|---|---|
| Sensing |  |
| Actuation |  |
| Wireless comunication |  |

## C. *Visual Grammar*

To define how visual elements can be joined to build a representation of a system, interaction rules must be specified. The collection of rules and the set of visual elements establish a visual grammar.

A straight black line between the objects denotes a communication channel. In the case of communication between two IoT devices, the line begins at the transmitter transceiver symbol and ends at the receiver transceiver symbol. The network protocol of this communication is indicated with a label on the line. If this protocol has a lock symbol at the beginning of the tag, then the communication between these objects is considered as encrypted.

TABLE III. VISUAL ELEMENTS OF SENSING INPUTS OF IOT SENSORS.

| Physical input | Visual element |
|---|---|
| Temperature |  |
| Moisture |  |
| Light |  |
| Heart rate |  |
| Presence |  |

TABLE IV. VISUAL ELEMENTS FOR SOME IOT ACTUATORS.

| Actuator | Visual element |
|---|---|
| Water pump |  |
| Electric relay |  |
| Oven |  |
| Light bulb |  |

To simplify and avoid an excessive number of communication lines of the same protocol between a single

receiving device and multiple sending devices, a black rectangle is placed. On one side of this rectangle, a single line is connected to the receiving device from the black rectangle. On the other side, several lines are drawn from all sources to the black rectangle. In other words, this black rectangle notation works like a multiplexer (although it is not a multiplexer, and the representation is just for visual purposes).

TABLE V. VISUAL ELEMENTS FOR COMMON IOT DEVICES.

| IoT device | Visual element |
|---|---|
| Gateway | |
| Cloud | |
| Development platform | |
| Microcontroller | |
| Smartphone | |
| Laptop | |

TABLE VI. VISUAL ELEMENTS FOR CYBERSECURITY REQUIREMENTS.

| Cybersecurity requirements | Visual element |
|---|---|
| Physical protection | |
| Encrypted comunication | |
| Encryption | |
| Decryption | |

## IV. SMART HOME USE CASES

To test the usability of the proposed visual elements and their grammar, we have represented some intelligent domestic IoT systems, taken from Kolias et al. [12]. These IoT systems consist of simple components, but they allow to demonstrate how stakeholders can use the elements proposed in this work to create visual representations of IoT systems and their cybersecurity requirements.

The first system discussed by Kolias is a custom lighting system for the smart home. The author illustrates the operation of the system with the image shown in Fig. 1, which is reproduced here from Kress and Leeuwen [10]. This system is built with the following hardware components: a Bluetooth beacon tag, a smart system bridge with Wi-Fi and Bluetooth transceiver, a computer with Wi-Fi and Bluetooth transceivers, a smartphone, and Bluetooth smart bulbs.

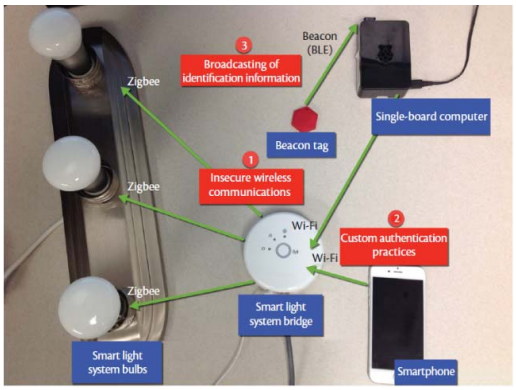


Fig. 1. An improvised representation of the IoT personalized light switch system components and interactions illustrated in Kress and Leeuwen [10, Fig. 1].

The Bluetooth tag constantly emits a beacon signal that can be detected by a computer to detect the presence of the user in the area. The user can configure and send orders to the light bulbs through an application that sends HTTP commands through a gateway. A database of user preferences can be stored in the computer memory.

In its security analysis, Kolias et al. [12] point out some security concerns for this system, such as insecure wireless communications, custom authentication practices for each manufacturer and the transmission of user information that has consequences for its privacy. Then an improvised representation of the interaction of components within the IoT system is performed, which cannot provide enough information about the communication between each device. The representation of this system using the proposed visual elements and the grammar is shown in Fig. 2. We can deduce additional information from the representation made with the visual elements, such as the type of device (IoT or not IoT), its function (sensor, actuator, both, etc.) or the type of environment variable it monitors. The abstraction of these device properties and their relationships allows a better understanding of their functionality among the system.

Additional visual elements, such as the lock icon, are used to indicate encryption and decryption processes within the components of the IoT system. These types of security features cannot be represented in a diagram without a visual element of specific purpose. The addition of visual elements to represent encryption communications facilitates the identification of insecure communications.

The second system considered consists of a remote irrigation system that uses the following commercial hardware components: an open source electronic platform (Arduino Uno), an Arduino Wi-Fi Shield, a Wi-Fi electrical relay, a small water pump, a photoelectric sensor, a humidity sensor, a temperature sensor, and a Wi-Fi hotspot. The representation of

the interaction between these devices made by Kolias can be seen in Fig. 3. The sensor takes environmental readings and sends them to the Arduino board. The Arduino board is connected to a Wi-Fi shield designed to establish communication with the Wi-Fi access point. If the humidity level is low, then the Arduino board sends a Wi-Fi command to the relay to activate it and turn on the water pump. The sensor data is sent to a web application to monitor the status of the system and generate live feeds for the user.

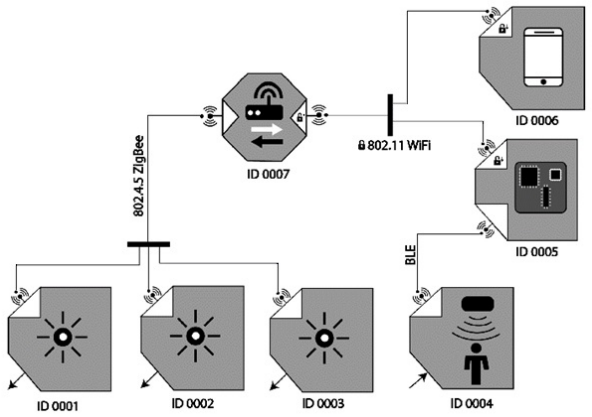


Fig. 2. Personalized light system representation made with the proposed visual elements and the visual grammar.

Once again, this system has vulnerabilities such as insecure web applications or lack of anti-spoofing and light encryption mechanisms.

The representation of this system with the proposed visual elements and grammar is shown in Fig. 4. One of the advantages of having a complete representation of the communications of the devices is that the route followed by the data of a device to reach another device can be deduced easily from the system diagram.

The last use case IoT system considered is an automatic control system to turn on/off potentially dangerous devices. The components used to build this system can be seen in Fig. 5 (used to represent the IoT system in [10]). The necessary devices for the construction of this system are a fitness tracker, a Wi-Fi electric smart switch, a Wi-Fi hotspot, a commercial cooker, and a smartphone.

The physical-activity tracker measures the user's current heart rate to infer their sleep status and send this data to an application installed on the smartphone. The function of the smartphone is to forward this data to a web application that executes an action when it is detected that the user carrying the tracker falls asleep.

The diagram for this system represented with the proposed visual elements is presented in Fig. 6. Once again, this system has the same Wi-Fi related vulnerabilities as the previous systems, such as the lack of encryption mechanisms and the manipulation of unprotected devices, as can be seen in the diagram. In general, each IoT system can rely on its cloud service counterparts, which opens a new entry point for cyberattacks.

In order to provide a more detailed information about the devices of an IoT system and to complement the representation made with the visual elements and the grammar, a table of properties is generated for each device. The table of an intelligent bulb is shown in Table VII. This table shows the properties of each IoT device that belongs to the system. The selection of attributes and properties is based on the papers presented by Ammar et al. [13], and Dorsemaine [14].

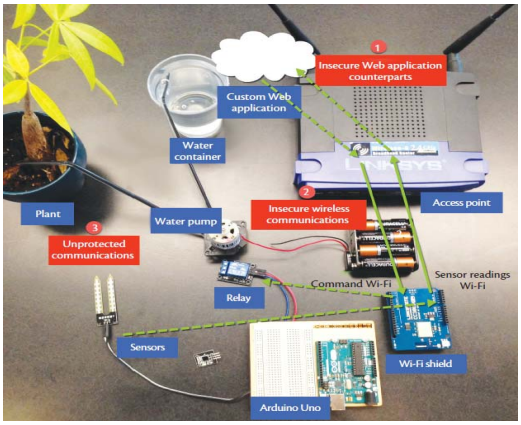


Fig. 3. An improvised representation of the IoT remote watering system components interactions illustrated in Kress and Leeuwen [10, Fig. 2].

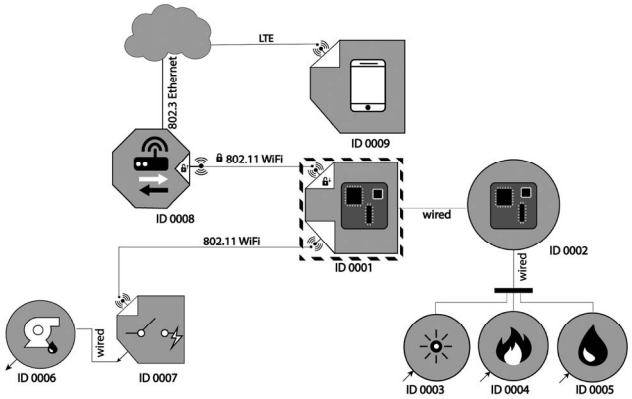


Fig. 4. An improvised representation of the IoT remote watering system components interactions illustrated in Kress and Leeuwen [10, Fig. 2].

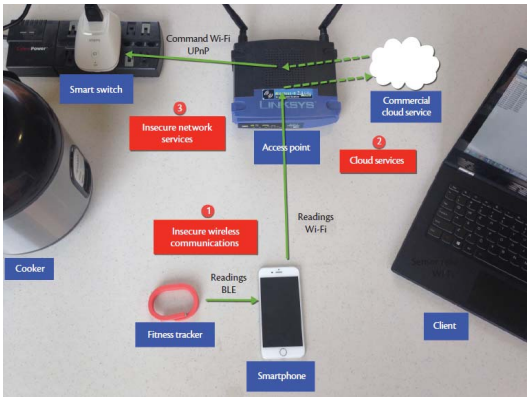


Fig. 5. An improvised representation of the IoT automatic on/off cooker system components interactions illustrated in Kress and Leeuwen [10, Fig. 3].

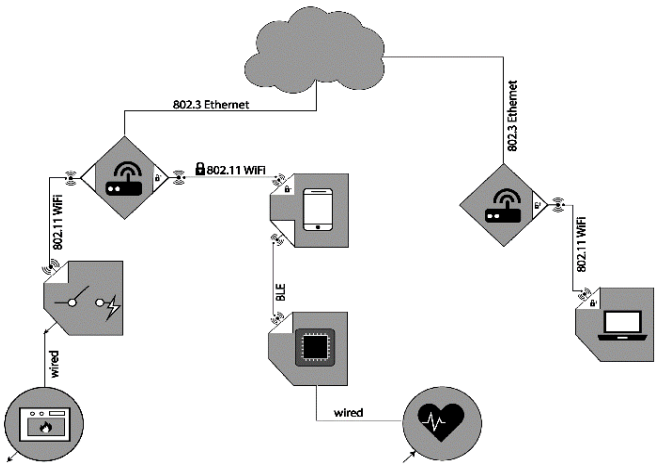


Fig. 6. Automatic on/off cooker system representation made with the proposed visual elements and the visual grammar.

TABLE VII. PROPERTIES OF SMART LIGHT BULB.

| | Properties | Value |
|---|---|---|
| General properties | Name | Smarth light bulb |
| | Identifier | 00001 |
| | Type | Actuator |
| | Mobility | Fixed |
| Software | Operating system | Unspecified |
| Hardware | RAM | Unspecified |
| | Memory | Unspecified |
| | Embedded sensors | No |
| | Embedded actuators | No |
| | Energy source | Mains powered |
| | Cryptographic module | No |
| Comunication | Type of comunication | Wireless |
| | Total disconection | No |
| | Initiation of communications | No |
| | Rate of transmission | 250 Kb/s |
| | Range | 30 meters |
| Comunication security | Authentication | No |
| | Identification | No |
| | Encryption | No |
| | Integrity | No |
| Protocols | Application layer comunication protocol | HTTP |
| | Network layer comunication protocol | Zigbee |
| Device Security | Authentication | Mutual |
| | Access Control | No |
| | Encryption | No |
| | Integrity | No |
| | Software updates | No |
| | User direct interaction | No |
| | Accountability | No |

## V. CONCLUSIONS AND FUTURE WORK

This paper presents the fundamentals of a visualization scheme to consider cybersecurity requirements in IoT systems. The objective of this proposal is to help security analysts identify the attack surfaces (and possibly attack vectors) of IoT systems and then apply cybersecurity controls to mitigate vulnerabilities. To improve the visual representation, more elements are being added considering other types of devices or technologies in different communication models and usage contexts. The general structure of a visual grammar has been defined to represent simple small systems in a smart home domain. To represent larger systems in other domains, more elements are being designed to consider different application scenarios in the IoT ecosystem.

A usability test will be carried out experimentally to test the visual representation obtained from the proposed visual elements and grammar. We will also investigate how visual representations can help to create misuse detection rules. Although the visual grammar design is still 'work in progress,' to our knowledge, this is the first time in which such kind of IoT visual representation has been proposed.

## ACKNOWLEDGMENT

This work was supported by Instituto Politécnico Nacional (IPN), Mexico, under project grants SIP-1999 and SIP-20200480; and by CONACYT under grant 264087.

## REFERENCES

[1] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the Internet of Things (IoT)," IEEE Internet Initiative, vol. 1, pp. 1-86, 2015.

[2] C. Greer, M. J. Burns, D. A. Wollman, E. R. Griffor, Cyber-Physical Systems and the Internet of Things. NIST Special Publication 1900-202, 2019.

[3] T. Eterovic, E. Kaljic, D. Donko, A. Salihbegovic, and S. Ribic, "An Internet of Things visual domain specific modeling language based on UML." In XXV International Conference on Information, Communication and Automation Technologies (ICAT). IEEE, 2015.

[4] D.A. Robles-Ramirez, P.J. Escamilla-Ambrosio, T. Tryfonas, "IoTsec: UML extension for internet of things systems security modelling." In IEEE International Conference on Mechatronics, Electronics and Automotive Engineering, 2017, Nov 21, pp. 151-156.

[5] O. Mavropoulos, H. Mouratidis, A. Fish, and E. Panaousis, "ASTo: A tool for security analysis of IoT systems." In IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA), London, 2017, pp. 395-400.

[6] O. Mavropoulos, H. Mouratidis, A. Fish and E. Panaousis, "Apparatus: A framework for security analysis in internet of things systems," Ad Hoc Networks, vol. 92, pp. 1-11, 2019.

[7] D. Basin, C. Cremers, and C. Meadows, "Model checking security protocols," in Handbook of Model Checking. Cham.: Springer, 2018, pp. 727-762.

[8] L. Wang, T. Islam, T. Long, A. Singhal, S. Jajodia, "An attack graph-based probabilistic security metric." In IFIP Annual Conference on Data and Applications Security and Privacy, 2008 Jul 13. Berlin, Heidelberg: Springer, pp. 283-296.

[9] M. Bauer, N. Bui, J. De Loof, C. Magerkurth, A. Nettsträter, J. Stefa, J.W. Walewski, "IoT reference model," in Enabling Things to Talk. Berlin: Springer, 2013, pp. 113-162.

[10] G. R. Kress and T. Leeuwen, Reading images: The grammar of visual design, Psychology Press, 1996.

[11] C. Nakamura and Q. Zeng-Treitler, "A taxonomy of representation strategies in iconic communication," International journal of human-computer studies, vol. 70, no. 8, pp. 535-551, Aug 2012.

[12] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, R. Kuhn, "Learning internet-of-things security "hands-on"," IEEE Security & Privacy, vol. 14, no. 1, pp. 37-46, Feb 2016.

[13] M. Ammar, G. Russello, B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications, vol. 38, pp. 8-27, 2018.

[14] B. Dorsemaine, J.P. Gaulier, J.P. Wary, N. Kheir, P. Urien, "Internet of Things: a definition & taxonomy." In IEEE 9th International Conference on Next Generation Mobile Applications, Services and Technologies Sep 2015, pp. 72-77.