Review Article

Johan Smith Rueda-Rueda* and Jesus M. T. Portocarrero

Framework-based security measures for Internet of Thing: A literature review

https://doi.org/10.1515/comp-2020-0220
Received Jul 08, 2020; accepted Dec 29, 2020

Abstract: This paper presents a review of state-of-the-art security frameworks for IoT applications. It aims to find out what alternatives have been proposed to guide IoT application developers in the implementation of security measures through all development phases. In this literature review, we identified 21 security frameworks, and we analyzed them from IoT application domains addressed and IoT elements protected. We find four application domains: generic, smart cities, smart car/VANET, and smart infrastructures. Concerning elements protected, we analyzed the frameworks through protected application resources and we also consider security properties in this paper. Our two principal findings are: (i) Even though there are a wide variety of security frameworks, we did not find a proposal that addresses all the layers of an IoT application (device, network, service and application) and all development phases (analysis, design, implementation, testing, deployment, and maintenance), (ii) Addressing security from the design phase allows IoT developers to have a broader perspective of the system, avoiding massive changes to be made in later stages, saving costs and time. This gap and concerns enable various research on security by design and secure development to be carried out, and proposed frameworks to address the identified problems.

Keywords: Cybersecurity, IoT application, security requirements, security framework, state-of-art

1 Introduction

Internet of Things – IoT, is a paradigm that is described as a network of physical and virtual objects (things), with embedded technology to communicate and detect or interact with their internal states or with the external environment [6, 28]. The IoT comprises an ecosystem that includes things, communications, applications, and data analysis, in which each object has an identification [45].

IoT has applications in sectors such as industrial processing, agriculture and breeding, logistic and product lifetime management, medical and healthcare, smart home/building, public safety, environmental monitoring, smart mobility, and smart tourism [9].

Mahalle and others [32] divide the challenges faced by the development of IoT applications into two categories: technological and security. The technological challenges refer to factors such as wireless communication, energy consumption, scalability, identification of sensor nodes, etc. The second group includes security, data privacy [5, 16, 29], resource trust [34, 47], identity management, end-to-end security, to name a few.

The security of an IoT application, as with any system, must be addressed throughout the development cycle. The system development cycle is guided by several development models, whether the traditional approach or agile development. These models include phases as planning, analysis, design, development, implementation, and maintenance. The analysis phase is where IoT application developers identify the functional requirements and quality or non-functional requirements. Security is a system quality requirement. In section 6, we go deeper into this aspect.

Managing the security of an IoT application must begin in the analysis and design phase. To consider security measures in these phases makes it easier for developers to have a more unobstructed view of what resources should be secured and how they should be secured. The above allows the IoT developers to design the security elements that will be required and to make better decisions during the application construction.

Several stakeholders are involved in the construction of an IoT application. Patel and Cassou [42] define five roles

***Corresponding Author: Johan Smith Rueda-Rueda:** Grupo de investigación en Tecnologías de Información. Universidad Autónoma de Bucaramanga. Bucaramanga, Santander. Colombia;
Email: jrueda526@unab.edu.co
Jesus M. T. Portocarrero: Professional services. Nuance Communications. Rio de Janeiro, JR. Brazil;
Email: jesus.talavera@nuance.com

involved in the development of IoT applications: domain expert, software designer, application developer, device developer, and network manager. These roles focus on one part in the design of an IoT application, and we do not identify a role that acts as an expert in information security issues.

One of the alternatives that IoT application developers can take is to use guides and good practices or frameworks that guide them on how and where to implement safety measures to protect their IoT application. A framework is a reusable design, either for a model or a source code, or both, that can be specialized and extended to provide a part of the general functionality of many applications [27].

The motivation for carrying out this research is that we did not find in the literature (review made until July 2020) any review or research on security frameworks for IoT focuses on the security concerns and the design phase of development. Section 2 shows other works that address security frameworks from different perspectives than ours. In addition, there are other proposals, such as reference architectures (RA), that guides IoT application developers in the building of IoT applications. Two of the most representative RAs in the literature are those proposed by the ITU-T [28] and the IoT-A Project [15], where security is not the primary purpose, neither it is widely addressed.

In this paper, we perform a literature review about proposed frameworks to guide or facilitate the implementation of security measures in IoT applications. The aim is to establish which domains those are oriented to, which resources they protect, and which phases of the development of IoT applications they address.

The remainder of the paper is organized as follows. Section 2 presents related works. Section 3 describes the methodology that guided this work. Section 4 presents the security frameworks for IoT proposed in the scientific literature. Section 5 discusses which IoT domains they address and which IoT resources they protected. Section 6 introduces the good practices of implementing security during the development of IoT applications. Finally, Section 7 presents the conclusions and identifies some research gaps.

2 Related Work

In this section, we present other literature review about security frameworks and explain how they differ from our work.

In [39], the authors provide an overview that includes security architecture frameworks, security and privacy issues, and a review of other studies on IoT security and privacy. Similarly, they present a taxonomy of attacks and their impact, the mitigations and countermeasures, and open research areas. The systematic review of [44] focuses on trust-based security frameworks.

The review in [25] addresses Information Security Frameworks, intending to facilitate organizations to carry out government strategies regarding the security of their assets and make decisions for their investment for secure IoT deployments. The authors analyze four frameworks, and they compare them according to the ISO 27001 standard.

The three related works are in line with ours in terms of introducing the reader to various security solutions for IoT. But what differentiates the papers is the focus of each research. The focus of [39] is to present multiple secure architectures, and urgent security and privacy concerns most relevant to IoT, and [44] focuses on one property of security, in particular, trust. Regarding [25], the focus is on information security and security risk management. Our focus is on the security frameworks that guide or facilitate the implementation of security measures in IoT applications on the design phase of development.

Numerous literature review papers address security in IoT. These works have focus on a wide variety of topics, among which are security challenges, security and privacy issues, cyber-attacks, and various proposals and technologies to address those. Also, there are security reviews for specific areas or domains such as smart homes, smart health, and smart cars among others.

3 Methods

The research question that addressed this literature review was the following: Is there a framework for security management in the design phase of an IoT application? To answer the question, we set two goals:

1. To know if there is a security framework that guides the implementation of security measures from the design phase of an IoT application.
2. To know which IoT resources and information properties are protected.

We performed a document search in two specialized databases, IEEE Xplorer and Scopus, using two groups of keywords: 'security model' OR 'security framework' AND 'Internet of Things' OR IoT.

As search criteria, we consider documents since the year 2010, and as document type, we include the conference proceedings and papers.

We applied the database search and downloaded the metadata of 56 documents. After reading the abstract of the articles, applying the quality criteria, we obtained 21 primary documents to proceed with for the data extraction.

For data extraction, we established two categories: (i) framework overview – name, application domain, goal, development cycle phase addressed, (ii) framework's target – information security properties and protected resources.

4 Security Frameworks

In this section, we introduce the IoT security frameworks proposed in the literature.

Atamli and Martin [4] propose a threat model based on use-cases of IoT. IoT application developers can use this model for determining where they invest efforts to secure the IoT systems.

Bohli *et al.* [8] propose Secure and sMARter ciTIEs data management (SMARTIE), a framework that follows a data-centric paradigm. SMARTIE is a platform for securing sensors and devices, for enabling resource access control, and providing secure data storage and processing capabilities in smart city applications.

Chen *et al.* [11] introduce ACSM, a cybersecurity management approach composed of various model-based various techniques. The ACSM aim is to protect networked computing systems from cyber adversaries.

Condry and Nelson [14] present a model scalable and resilient, which aims to protect communications between IoT clients and the Gateway device. This solution employs computational, cryptography, signal/image processing, and communication capabilities for authentication and authorization functions.

Ge and Kim [19] present a framework for security modeling and assessment of the IoT, whose main objectives are: (i) describe all possible attack paths; (ii) assess the level of IoT security through security metrics, and (iii) evaluate the effectiveness of defense strategies. The proposed framework consists of five phases: data processing, security model generation, security visualization, security analysis, and model updates.

Hellaoui *et al.* [22] introduce TAS-IoT, a model for adaptive security based on trust management. TAS-IoT consists of two algorithms to authenticate the message according to the confidence level it associates with the sender of the message. This adaptive security solution aims to reduce authentication overhead by using packet authentication only when required.

Hernandez-Ramos *et al.* [23] propose a set of lightweight authentication and authorization mechanisms to support intelligent objects during their life cycle. It aims to provide a comprehensive safety approach that takes advantage of the design of new, lightweight safety protocols for restricted environments for IoT.

Huang *et al.* [24] introduce SecIoT, a framework that includes: authentication mechanisms, a flexible role-based access system and a security risk indicator interface. SecIoT aims to help users understand and control the system security risks; and provides essential authentication, secures communications, supports user authorization, and notifies of potential risks.

Liu *et al.* [30] propose AEC, a framework to verify protocol authentication using Communicating Sequential Processes (CSP). CSP is a formal language to describe interaction patterns in concurrent systems. This framework includes three forms of authentication: entity authentication, action authentication, and claim authentication.

Lize *et al.* [20] establish a formal trust management control mechanism based on the architecture modeling of IoT. The authors decompose the IoT domain into the sensor layer, core layer, and application layer. Each of these layers is controlled by a trust management for a particular purpose, namely: self-organized, for the sensor layer, effective routing for the core layer, and multi-service for the application layer. The service requester performs the final decision-making according to the collected trust information as well as the requester's policy.

Mozzaquatro *et al.* [35] propose IoTSec, a reference ontology for IoT security, in order to help find secure solutions to the IoT environment. Authors designed IoTSec based on information security issues that can be represented using structured knowledge. IoTSec unifies concepts and clarifies relationships among different terms, to provide an overview of the domain of security in IoT.

Namal *et al.* [36] propose an autonomic trust management framework for web-based IoT applications and services. This framework is based on the MAPE-K reference model. This framework makes use of the MAPE-K feedback control loop to evaluate the level of confidence in an IoT cloud ecosystem.

Neisse *et al.* [37] present SeKit, a model-based Security Toolkit, focused on all layers of the iCore Framework. SeKit is a collection of metamodels that provides the basis for security engineering tooling, add-ons, runtime components, and extensions to address security, data protection, and privacy requirements.

Pacheco and Hariri [40] propose and IoT Security Framework. This framework has two purposes: to guide the development of intelligent IoT infrastructure security and to identify potential vulnerabilities and the appropriate mitigation mechanisms.

Pacheco *et al.* [41] propose an IoT Security Development Framework (ISDF). Developers can be ISDF to consider security issues at all IoT layers and integrate security algorithms with the functions and services offered in each layer, rather than considering security in an ad-hoc and afterthought manner. The main objective is to provide the architectural support to develop highly secure and reliable IoT services that can proactively detect and tolerate malicious damage that may be due to attacks, malicious or natural failures and accidents.

Radomirovic [43] proposes a model consisting of an asynchronous communication network and a Dolev-Yao opponent with fingerprinting skills, distinguishing between mobile and static devices. For the author, to reason about security and privacy, IoT must be considered as a fusion of the operating system and a network, where incoming and outgoing items as well as private space itself need to be scanned for fraudulent devices and malware.

Serna *et al.* [46] present a framework that addresses security and privacy issues in the Vehicular Ad-Hoc Network (VANET). The proposed framework consists of three elements: (i) an inter-domain authentication system capable of providing a near real-time certificate status service; (ii) a mechanism to quantitatively evaluate the trust level of a Certificate Authority and to establish an on-the-fly inter-operability relationship, and (iii) a privacy-enhancing model that addresses privacy in terms of linkability.

Singh and Bhandari [48] propose Network Security Situational Awareness (NSSA), a semantic web-based framework for situational awareness network security. These authors address issues with a traditional network security approach. These issues require a formal model to represent entities in a network which should have the ability to accommodate new entities, represent the relationships between entities and also adapt to changes in the network configuration.

Tahir *et al.* [49] present ICMKeyStream, a framework for protecting against threats at the device layer and network layer. It use elements ICMetric and Secure Remote Rabbit Protocol. It aims to secure the entities and their intercommunications. Also, providing security for the IoT, authentication, confidentiality, and non-repudiation for continuous data flow.

Yang and Fang [51] analyze the IoT linkage between communication, control, and computation. The authors propose a security framework for control and computation. This proposal considers the following aspects: architecture security, terminal security, transport security, control security, privacy protection, security management, method, and evaluation mechanisms.

Zegzhda and Stepanova [52] present a theoretical framework to tackle security threats, aimed at disrupting, degrading, or destroying IoT components and services. The authors propose a finite state model of the behavior of an IoT agent, which is oriented to the development of IoT applications within the network layer specifically. It aims to maintain adaptive topological sustainability in a hostile environment. To that end, it uses a hybrid architecture with reallocatable control centers and the balance of the number of links between IoT entities.

5 Analysis of the proposed security frameworks

To analyze the security framework found in the literature, we focus on two aspects: (i) which IoT application domains the security frameworks are oriented to and (ii) which elements of the IoT domain they are protecting.

5.1 Security Framework Application Domains

In the first focus of analysis, we identified four application domains of the 21 frameworks analyzed. 76,19% of the frameworks are proposed for generic IoT applications, regardless of the application domain. The remaining frameworks have been proposed for the following application domains: smart cities and Smart Car/VANET, with 9,52%, and smart infrastructures with 4,76% representation. In Figure 1, we present the security framework organized by application domains.

The significant tendency towards security frameworks for generic applications is because this type of proposal applies to the general requirements of any application domain. Examples of these requirements are device management, data transfer, data processing and storage, data analysis, and data visualization, to name a few. In this sense, IoT developers can use these security proposals in an IoT application in the fields of health, smart home, industrial, among others.

On the other hand, the reason to propose a framework for a particular domain is that it addresses the specific requirements of this particular domain. These differences may be perceived in one or more of the layers of an IoT application.

Of the frameworks analyzed, we identified that the proposed ones by Pacheco and Hariri [40] for smart infrastruc-

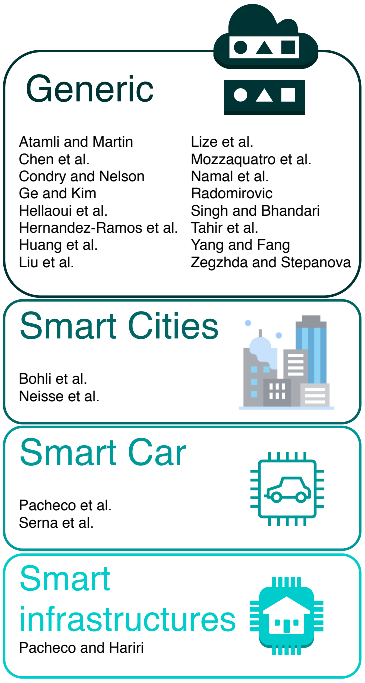


Figure 1: Security Framework Application Domains

tures domain and Pacheco *et al.* [41] for smart car/VANET domain have similar four-layer architectures. The difference between the two is in the network layer. In the network layer, the framework for smart infrastructures has a gateway for transmission of information from/to end nodes. On the other hand, the framework for smart car/VANET has several protocols for communication of the internal and external networks.

The proposal by Serna *et al.* [46] is an example of a framework for a specific domain. Authors confirm that authentication protocol in a VANET system must cope with the specifics introduced by different scenarios: vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V).

The smart cities' proposals also have differences. The Bohli *et al.* [8] framework addresses the generic smart city, but it focuses on protecting sensors and devices, enables access control for resources, and providing secure data storage and processing. The Neisse *et al.* [37] proposal integrates with a specific solution, the iCore Framework.

5.2 IoT elements protected by the frameworks

For the second focus of analysis, we present the results from two perspectives: (i) according to the layer where the protected IoT resources are located, and (ii) according to the information security property they safeguard or the security mechanism they use.

5.2.1 Protected IoT resources

The architecture of an IoT application can vary according to the level of abstraction performed by its authors. The most common architectural style is layers. In the literature have been proposed three-layers architecture to seven-layer architectures. Para this analysis, we use the ITU-T IoT reference model [28], consisting of four layers, as shown in Figure 2.

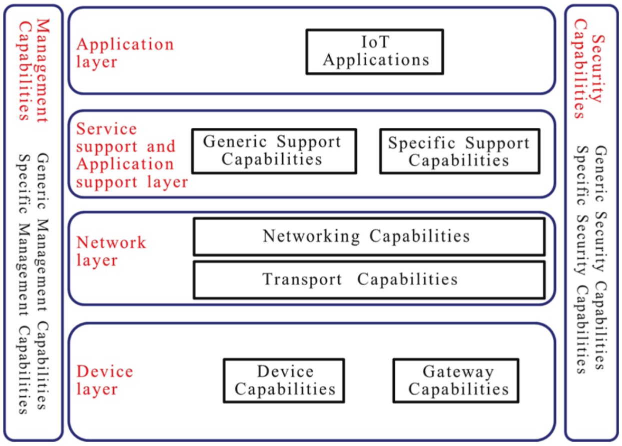
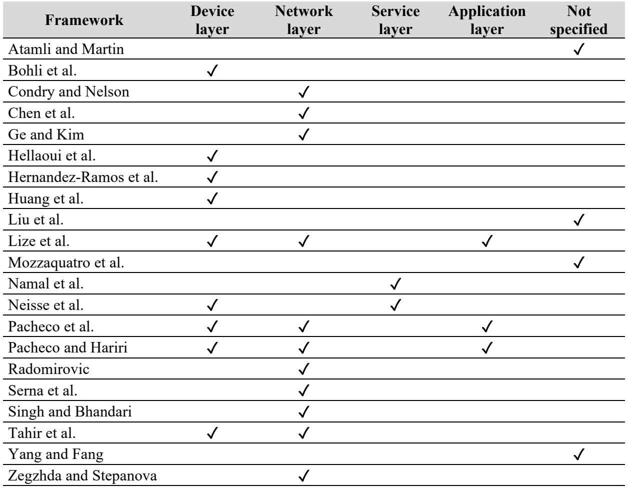

Management Capabilities
Generic Management Capabilities
Specific Management Capabilities
Application layer
IoT Applications
Service support and Application support layer
Generic Support Capabilities
Specific Support Capabilities
Network layer
Networking Capabilities
Transport Capabilities
Device layer
Device Capabilities
Gateway Capabilities
Security Capabilities
Generic Security Capabilities
Specific Security Capabilities

Figure 2: ITU-T IoT reference model [28]

Once we have identified the protected IoT resources by each security framework, we organize every proposal in the layer or layers that they address, according to the IoT reference model. Additionally, we have added a fifth field to classify those frameworks where it was not clear which resources or layers the solution is oriented towards. Figure 3 shows the results.

As shown in Figure 3, 57% of the frameworks are addressed to one layer. Of this fraction, 58% focus on the network layer, 34% focus on the device layer, and 8% focus on the service layer. Secondly, frameworks addressed to three layers represent 14%. The proposal by [20, 40, 41] are focused on the device layer, network layer, and service layer.

The 10% of the proposals deal with frameworks addressed to two layers. The proposal by [37] focuses on the device layer and service layer, and the proposition by [49] targets the device layer and network layer. The remaining 19% of the frameworks that do not clearly explain the layer(s) they address.

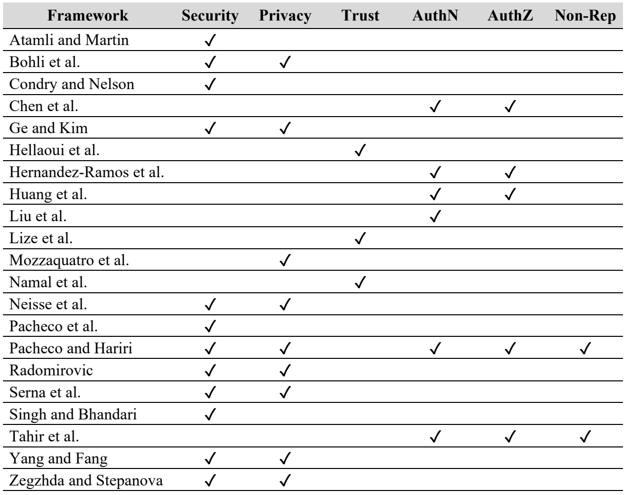


Framework	Device layer	Network layer	Service layer	Application layer	Not specified
Atamli and Martin					✓
Bohli et al.	✓				
Condry and Nelson		✓			
Chen et al.		✓			
Ge and Kim		✓			
Hellaoui et al.	✓				
Hernandez-Ramos et al.	✓				
Huang et al.	✓				
Liu et al.					✓
Lize et al.	✓	✓		✓	
Mozzaquatro et al.					✓
Namal et al.			✓		
Neisse et al.	✓		✓		
Pacheco et al.	✓	✓		✓	
Pacheco and Hariri	✓	✓		✓	
Radomirovic		✓			
Serna et al.		✓			
Singh and Bhandari		✓			
Tahir et al.	✓	✓			
Yang and Fang					✓
Zegzhda and Stepanova		✓			

Figure 3: IoT resources protected by the security frameworks

5.2.2 Security properties considered

To guarantee the security of the data and the entire IoT system, IoT application developers should consider the confidentiality, integrity, and availability of the information [13, 21]. Concerning data protection, we identified that frameworks addressed one or more of the following security properties: security, privacy, trust, authentication (AuthN), authorization (AuthZ), and non-repudiation (Non-Rep). Figure 4 shows a summary of the analysis carried out.



Framework	Security	Privacy	Trust	AuthN	AuthZ	Non-Rep
Atamli and Martin	✓					
Bohli et al.	✓	✓				
Condry and Nelson	✓					
Chen et al.				✓	✓	
Ge and Kim	✓	✓				
Hellaoui et al.			✓			
Hernandez-Ramos et al.				✓	✓	
Huang et al.				✓	✓	
Liu et al.				✓		
Lize et al.			✓			
Mozzaquatro et al.		✓				
Namal et al.			✓			
Neisse et al.	✓	✓				
Pacheco et al.	✓					
Pacheco and Hariri	✓	✓		✓	✓	✓
Radomirovic	✓	✓				
Serna et al.	✓	✓				
Singh and Bhandari	✓					
Tahir et al.				✓	✓	✓
Yang and Fang	✓	✓				
Zegzhda and Stepanova	✓	✓				

Figure 4: Security properties addressed by the security frameworks

Security and privacy are two properties that are closely related. Security is a condition that results in implementing and maintaining protection measures to secure data or information assets, guaranteeing confidentiality, integrity, and availability. Privacy is the protection given to information to safeguard it from unauthorized intrusion or disclosure.

Authentication and authorization are also closely related. While authentication validates the identity of the user or thing who wishes to enter the system or interact with it, authorization determines what permissions that user or thing has within the system.

5.3 Discussion of the analysis

In this sub-section, we present the main findings by comparing the results of sub-section 4.1 and 4.2.

Security and privacy are the most addressed properties in all the application domains presented in Figure 1. The two proposed frameworks for smart cities address these two properties. The security and privacy of data collected by applications and services are one of the major concerns of citizens and governments and the main challenges for them to accept such technologies.

Security and privacy are critical in other domains. The smart car and smart infrastructure applications are very much related to people's personal lives. They are saturated with personal data, data on the private environment, frequent places and routes, and much more.

Analyzed frameworks address the protection measures to ensure security and privacy on all layers described in Figure 2. Still, most of them mainly focus on the device layer, network layer, and application layer.

All frameworks that address trust focus on the device layer. Concerning authentication and authorization, frameworks that address these properties are mainly focused on the device layer and network layer.

Frameworks that consider the non-repudiation, focus their efforts on the device and network layer.

The most robust framework is the one proposed by [40] since it addresses the device, network, and application layers, and it considers the properties of security, privacy, authentication, authorization, and non-repudiation. But this framework addresses one particular application domain, smart infrastructures.

Cybersecurity risks are a real issue that is impacting organizations and home users. For an organization, the impact of a cybersecurity breach can be reflected in damaging the reputation, theft, financial losses, fines, and several intangible costs [3, 18].

A study on cyber risk in smart homes, in which 16 million home networks were scanned, indicates that 40.8% have at least one vulnerable connected device, "as it only takes one vulnerable device to compromise the security of the whole home network" [7]. Another study on security risks in business environments indicates that the IoT devices evaluated can be hacked in as little as three minutes, but it can take days or weeks to remedy these incidents [50].

The data mentioned above highlight the actual need for utilizing some IoT security proposals. But the decision to use a security framework that guides or facilitates the implementation of security measures implies other considerations on the part of the development team. Factors such as how critical the data is that the IoT application is going to generate, transport, and store; not all data and information assets require the same security measures. Another consideration is how large and distributed the system that is about to be built is. Similarly, if the development team has expert roles, it is a cybersecurity or a security engineer who guides them in the secure development of IoT applications.

In this sense, development teams can decide between two approaches: (i) to use a framework that covers the entire domain of cybersecurity in IoT, or (ii) a framework that addresses a specific mechanism of IoT security. The frameworks studied in this work are examples of the proposed ones that address security-specific mechanisms. A third alternative are proposals that guide the implementation of good practices, such as user authentication [38], communication encryption oriented to IoT devices [2], to name a few.

6 Desirable security in building IoT applications

Security is a quality requirement and a cross-cutting of any system [1, 26]. The implementation of security measures in IoT applications can be perceived from two perspectives. In the first of these, the application development team considers security measures in the analysis and design phase of the system. In the second, the development team focuses on the functional requirements, and the security measures are considered during the construction process of the application or after completing all development phases.

An adequate analysis of the quality requirements is fundamental for the development process of the IoT application [12]. In the analysis phase, the development team determines the functional and quality characteristics to be met. Based on these characteristics, they will design, implement, and carry out tests on the system. If the quality requirements are not properly managed, any change in the later development phases will entail an increase in the design and implementation time and the cost [31]. For this reason, quality requirements are the most expensive and difficult to correct once the system has been implemented [10, 17].

To consider security measures in development phases makes it easier for developers to have a more unobstructed view of what IoT resources should secure and how they should be secured. This system view will allow the developers to choose the devices and additional hardware best suited to the functional and security requirements. Moreover, communication protocols with good layers of protection should be selected. These technologies must be compatible with the computing and energy consumption capabilities of the hardware chosen. Similarly, one has to decide on the software and applications that they will use in each processing layer, such as fog computing, edge computing, and cloud computing. In this way, one determines each hardware and software configuration and see security as a whole and not as separate parts of the same system.

A different approach could be that the development team focuses on the functional requirements and on solving some of the technical challenges such as computing capabilities, wireless communication, or energy consumption. Meeting the security requirements, if developers considered them at all, is done during the development of the IoT system or once you have a marketable product. The above described is in response to a market that demands solutions, with a growing competition where the differentiating factor in technologies is relevant.

For adequate data protection, developers must examine the application as a whole. From this view, applying the security measures to the whole and not consider the system as several individual elements, and of these elements, just to protect those they consider relevant, or they leave other components unprotected because they ignore the entirety of the system. There are no layers more critical than others; each IoT application layer is susceptible to security threats and attacks [33].

7 Conclusions, research gap and research opportunities

In this paper, we carried out a literature review on proposed frameworks to guide or facilitate the implementation of security measures in IoT applications. This literature review arises from the need for a work that will analyze the proposed contributions to guide IoT application developers on how to secure their applications. This review of the state-of-the-art is the first contribution of this research work.

We analyzed the security frameworks focused on two aspects: the application domains they address and the resources they protect. Likewise, we approached good practice in the implementation of security measures in the development of IoT applications.

The security frameworks are proposed for generic, smart cities, smart car/VANET, and smart infrastructure domains; they consider one or more layers of an IoT application, and in tandem, they consider security, privacy, trust, authentication, authorization, and non-repudiation. Proposed frameworks mainly address the device layer and the network layer and the properties of security and privacy.

In the literature, we did not find a framework that addresses the device, network, service, and application layers, or security properties that are considered in this article. The most robust identified framework considers three of the four layers and five of the security properties. But this framework focuses on smart infrastructures.

There is both a research and a technical gap in the frameworks that guide developers in the implementation of security measures in all phases of building IoT applications. Besides, to address a generic approach one should consider all layers of an IoT application and most security properties.

This gap may be a result of the fact that security, as a cross-cutting domain of IoT, is not entirely figured out. IoT developers lack knowledge about which elements should be protected and how to address security challenges. Cybersecurity is an extensive area, and, also, the IoT paradigm involves many heterogeneous technologies making it challenging to treat safety comprehensively on the IoT.

Research opportunities arise on various topics within the identified gap. Some of the research topics that we highlight are: (i) a conceptual model that guides IoT application development teams on the security considerations they must take into account to secure their applications and systems; (ii) An ontological model or a model represented through semi-formal languages, such as Unified Modeling Language (UML), and formal ones that allow software architects to instantiate generic architectures in particular architectures of the applications they want to build.

The IoT paradigm is currently prevalent, together with other, so-called in academic and industrial circles, industry 4.0 technologies. Governments see it as an opportunity to develop strategic sectors of their countries, contributing to productivity and wealth generation and improving the standard of living of their citizens. Proposing a framework with the considerations mentioned above becomes relevant and necessary for the development of the IoT since security problems can be a factor that generates a delay in the implementation of these solutions in the home, industry, and city contexts.

Conflict of interest: Authors state no conflict of interest.

References

[1] Adams K. M. et al., Nonfunctional requirements in systems analysis and design, 2015, 28, Springer.

[2] Alassaf N., Gutub A., Parah S. A., Al Ghamdi M., Enhancing speed of simon: A light-weight-cryptographic algorithm for iot applications, Multimedia Tools and Applications, 2019, 78(23), 32633–32657.

[3] AS S., The consequences of a cyber security breach, 2018.

[4] Atamli A. W. Martin A., Threat-based security analysis for the internet of things.

[5] Atzori L., Iera A., Morabito G., The internet of things: A survey, Computer networks, 2010, 54(15), 2787–2805.

[6] Atzori L., Iera A., Morabito G., Understanding the internet of things: definition, potentials, and societal role of a fast evolving paradigm, Ad Hoc Networks, 2017, 56, 122–140.

[7] Avast, Avast smart home security report 2019, 2019, Technical report.

[8] Bohli J.-M., Skarmeta A., Moreno M. V., García D., Langendörfer P., Smartie project: Secure iot data management for smart cities, 2015 International Conference on Recent Advances in Internet of Things (RIoT), IEEE, 2015, 1–6.

[9] Borgia E., The internet of things vision: Key features, applications and open issues, Computer Communications, 2014, 54, 1–31.

[10] Brooks F. P., Essence and accidents of software engineering, IEEE Computer, 1997, 20(4).

[11] Chen Q., Abdelwahed S., Erradi A., A model-based validated autonomic approach to self-protect computing systems, IEEE Internet of things Journal, 2014, 1(5), 446–460.

[12] Chung L., Nixon B. A., Yu E., Mylopoulos J., Non-functional requirements in software engineering, 2012, 5, Springer Science & Business Media.

[13] Cirani S., Ferrari G., Veltri L., Enforcing security mechanisms in the ip-based internet of things: An algorithmic overview, Algorithms, 2013, 6(2), 197–226.

[14] Condry M. W. Nelson C. B., Using smart edge iot devices for safer, rapid response with industry iot control operations, Proceedings of the IEEE, 2016, 104(5), 938–946.

[15] CORDIS, Internet of things architecture, 2019.

[16] Da Xu L., He W., Li S., Internet of things in industries: A survey, IEEE Transactions on industrial informatics, 2014, 10(4), 2233–2243.

[17] Davis A. M., Software requirements: objects, functions, and states, 1993, Prentice-Hall, Inc.

[18] Deloitte, Business impacts of cyber attacks, 2018.

[19] Ge M., Hong J. B., Guttmann W., Kim D. S., A framework for automating security analysis of the internet of things, Journal of Network and Computer Applications, 2017, 83, 12–27.

[20] Gu L., Wang J., Sun B., Trust management mechanism for internet of things, China Communications, 2014, 11(2), 148–156.

[21] Heer T., Garcia-Morchon O., Hummen R., Keoh S. L., Kumar S. S., Wehrle K., Security challenges in the ip-based internet of things, Wireless Personal Communications, 2011, 61(3), 527–542.

[22] Hellaoui H., Bouabdallah A., Koudil M., Tas-iot: trust-based adaptive security in the iot, 2016 IEEE 41st Conference on Local Computer Networks (LCN), IEEE, 2016, 599–602.

[23] Hernandez-Ramos J. L., Pawlowski M. P., Jara A. J., Skarmeta A. F., Ladid L., Toward a lightweight authentication and authorization framework for smart objects, IEEE Journal on Selected Areas in

Communications, 2015, 33(4), 690–702.

[24] Huang X., Craig P., Lin H., Yan Z., Seciot: a security framework for the internet of things, Security and communication networks, 2016, 9(16), 3083–3094.

[25] Irshad M., A systematic review of information security frameworks in the internet of things (iot), 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), IEEE, 2016, 1270–1275.

[26] ISO/IEC, Iso/iec 25010:2011 systems and software engineering – systems and software quality requirements and evaluation (square) – system and software quality models, 2011, Technical report, Technical Committee : ISO/IEC JTC 1/SC 7 Software and systems engineering.

[27] ISO/IEC/IEEE, Iso/iec/ieee 24765:2017 systems and software engineering – vocabulary, 2017, Technical report, Technical Committee: ISO/IEC JTC 1/SC 7 Software and systems engineering.

[28] ITU-T, Y.2060: Overview of the internet of things, 2012, Technical report, International Telecommunication Union.

[29] Lee I. Lee K., The internet of things (iot): Applications, investments, and challenges for enterprises, Business Horizons, 2015, 58(4), 431–440.

[30] Liu L., Yin L., Guo Y., Fang B., Eac: a framework of authentication property for the iots, 2014 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, IEEE, 2014, 102–105.

[31] Mahalank S. N., Malagund K. B., Banakar R., Non functional requirement analysis in iot based smart traffic management system, 2016 International Conference on Computing Communication Control and automation (ICCUBEA), IEEE, 2016, 1–6.

[32] Mahalle P. N., Anggorojati B., Prasad N. R., Prasad R., Identity authentication and capability based access control (iacac) for the internet of things, Journal of Cyber Security and Mobility, 2013, 1(4), 309–348.

[33] Mahmoud R., Yousuf T., Aloul F., Zualkernan I., Internet of things (iot) security: Current status, challenges and prospective measures, 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, 2015, 336–341.

[34] Miorandi D., Sicari S., De Pellegrini F., Chlamtac I., Internet of things: Vision, applications and research challenges, Ad hoc networks, 2012, 10(7), 1497–1516.

[35] Mozzaquatro B. A., Jardim-Goncalves R., Agostinho C., Towards a reference ontology for security in the internet of things, 2015 IEEE International Workshop on Measurements & Networking (M&N), IEEE, 2015, 1–6.

[36] Namal S., Gamaarachchi H., MyoungLee G., Um T.-W., Autonomic trust management in cloud-based and highly dynamic iot applications, 2015 ITU Kaleidoscope: Trust in the Information Society (K-2015), IEEE, 2015, 1–8.

[37] Neisse R., Fovino I. N., Baldini G., Stavroulaki V., Vlacheas P., Giaffreda R., A model-based security toolkit for the internet of things, 2014 Ninth International Conference on Availability, Reliability and Security, IEEE, 2014, 78–87.

[38] Nespoli P., Zago M., Huertas Celdrán A., Gil Pérez M., Gómez Mármol F., García Clemente F. J., Palot: profiling and authenticating users leveraging internet of things, Sensors, 2019, 19(12), 2832.

[39] Obaidat M. A., Obeidat S., Holst J., Al Hayajneh A., Brown J., A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures, Computers, 2020, 9(2), 44.

[40] Pacheco J. Hariri S., Iot security framework for smart cyber infrastructures, 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W), IEEE, 2016, 242–247.

[41] Pacheco J., Satam S., Hariri S., Grijalva C., Berkenbrock H., Iot security development framework for building trustworthy smart car services, 2016 IEEE Conference on Intelligence and Security Informatics (ISI), IEEE, 2016, 237–242.

[42] Patel P. Cassou D., Enabling high-level application development for the internet of things, Journal of Systems and Software, 2015, 103, 62–84.

[43] Radomirovic S., Towards a model for security and privacy in the internet of things, Proc. First Int'l Workshop on Security of the Internet of Things, 2010.

[44] Rana K., Singh A. V., Vijaya P., A systematic review on different security framework for iot, 2018 Fifth International Symposium on Innovation in Information and Communication Technology (ISIICT), 2018, 1–7.

[45] Rueda J. S. Portocarrero J. M. T., Similitudes y diferencias entre redes de sensores inalámbricas e internet de las cosas: Hacia una postura clarificadora, Revista Colombiana de Computación, 2017, 18(2), 58–74.

[46] Serna J., Morales R., Medina M., Luna J., Trustworthy communications in vehicular ad hoc networks, 2014 IEEE World Forum on Internet of Things (WF-IoT), IEEE, 2014, 247–252.

[47] Sicari S., Rizzardi A., Grieco L. A., Coen-Porisini A., Security, privacy and trust in internet of things: The road ahead, Computer networks, 2015, 76, 146–164.

[48] Singh M. Bhandari P., Building a framework for network security situation awareness, 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, 2016, 2578–2583.

[49] Tahir R., Tahir H., McDonald-Maier K., Fernando A., A novel icmetric based framework for securing the internet of things, 2016 IEEE International Conference on Consumer Electronics (ICCE), IEEE, 2016, 469–470.

[50] Technologies F., Know your iot security risk. how hackable is your smart enterprise?, 2016, Technical report.

[51] Yang J.-C. Fang B.-X., Security model and key technologies for the internet of things, The Journal of China Universities of Posts and Telecommunications, 2011, 18, 109–112.

[52] Zegzhda D. Stepanova T., Achieving internet of things security via providing topological sustainability, 2015 Science and Information Conference (SAI), IEEE, 2015, 269–276.