Towards an Assurance Framework for Edge and IoT Systems

Marco Anisetti*, Claudio A. Ardagna*, Nicola Bena* and Ruslan Bondaruc*
*Department of Computer Science
Università degli Studi di Milano
Milan, Italy
Email: {firstname.lastname}@unimi.it, ruslan.bondaruc@studenti.unimi.it

***Abstract*—Current distributed systems increasingly rely on hybrid architectures built on top of IoT, edge, and cloud, backed by dynamically configurable networking technologies like 5G. In this complex environment, traditional security governance solutions cannot provide the holistic view needed to manage these systems in an effective and efficient way. In this paper, we propose a security assurance framework for edge and IoT systems based on an advanced architecture capable of dealing with 5G-native applications.**

***Index Terms*—Assurance, Cloud-Edge, IoT, Security, Kubernetes**

I. Introduction

The last few years have experienced the emergence of new computing paradigms, namely edge and IoT, grounded on novel low-latency communication protocols such as 5G. Edge and cloud computing are the enabling technologies for IoT, as devices constantly send and receive data to the upper layers. Together, these paradigms paved the way to groundbreaking sensor-based smart services that are disruptively shaping our lives, with 29.3 billion of connected devices estimated by 2023 [1] and a range of 2.7 trillion to 6.2 trillion dollars of economic impact estimated by 2025 [2]. Notwithstanding the huge benefits these systems are bringing to our lives, such a pervasiveness can introduce new and serious threats, which need to be considered and properly mitigated. Security, privacy, and safety are crucial aspects to carefully tackle, and guaranteeing resilience, robustness and, in general, the correct behavior of such systems is a more-than-ever pressing need.

In particular, security assurance stands out as the mean to address such need. Being consistently applied to traditional distributed systems (e.g., services, cloud [3]), assurance techniques now fall short when facing the new challenges raised by hybrid edge and IoT systems, in terms of scalability and ability to adapt to dynamic, complex yet resource-constrained systems [4]. Conventional security assurance techniques fail in evaluating the target system as a whole and do not consider new mobile networks, like 5G, demanding a complete rethink of existing practices. Such a rethink affects both the methodological and the practical point of view, that is, assurance frameworks implementing those practices. While some solutions have been already proposed, e.g., [5], they are far from being fully comprehensive.

Our paper aims to address the above gaps by defining a novel security assurance framework for cloud/edge and IoT systems. It implements a highly scalable assurance process that guarantees trustworthy non-functional properties by collecting relevant evidence on the target systems. It follows a distributed cloud/edge architecture implemented on Kubernetes, with automatic scaling and high availability. In short, our framework enables new generation assurance activities in edge and IoT infrastructures, regardless of their complexity and size.

The contribution of our work is twofold. We first highlight the challenges of edge and IoT assurance, and define the corresponding requirements to fill them in (Section II). We then introduce our proposed assurance framework (Section III) and a real-world use case (Section IV).

II. Challenges and Requirements

A. Challenges

Security assurance is defined as the mean to obtain justifiable confidence that an IT system behaves as expected demonstrating some non-functional properties (e.g., confidentiality) [3]. In the last decade, assurance has become a well-established practice, increasing the trustworthiness of service and cloud systems [3], with some methodologies addressing hybrid clouds [6] and edge systems [5]. However, hybrid cloud/edge and IoT systems raise some significant challenges, impairing the effectiveness of state of art solutions. We summarize these challenges as follows.

- **Scale**. Typical edge/IoT scenarios have hundreds of nodes and devices deployed in different locations, requiring highly-scalable assurance processes and frameworks [7].
- **Lightness**. IoT devices are resource-constrained, calling for more lightweight assurance techniques while not giving up on the provided trustworthiness [4].
- **Dynamism**. Edge and IoT systems are dynamic by nature, as nodes enter and exit the system at a very high rate. Assurance solutions need to keep track of the state of a continuously evolving infrastructure, and punctual evaluations are no longer practical.
- **Heterogeneity**. Edge and IoT are not strictly-defined paradigms, as a plethora of standards, best practices

Research supported, in parts, by EC H2020 Project CONCORDIA GA 830927, Università degli Studi di Milano under the program "Piano sostegno alla ricerca", and GARR through the Orio Carlini scholarship 2020-2021.

and technologies do exist [8]. It is therefore difficult to properly assess those systems.
- **Unawareness**. IoT suffers from the shadow IT problem, demanding for assurance techniques assessing the target system as a whole, without precise knowledge.
- **Responsiveness**. Cloud, edge and IoT have deeply different response time in patching issues. Cloud updates in real-time, edge updates slowly, and IoT does not update at all. Assurance techniques should account for those differences to guarantee an appropriate effectiveness.

Addressing *scale* permits to adapt to large edge and IoT networks, while facing *lightness*, *heterogeneity*, and *unawareness* helps coping with the intrinsic design characteristics of IoT technology. *Dynamism* allows to deal with complex scenarios. Finally, *responsiveness* considers update times at different architectural levels.

B. Requirements

From the above challenges, it emerges that traditional assurance frameworks cannot be directly adapted for edge and IoT systems due to intrinsic and unresolvable gaps [9]. For instance, they struggle to adapt to the size of target systems and do not offer automated deployment solutions [10], to name but a few. In other words, a paradigm shift is needed. To this aim, we summarize the requirements that a security assurance framework for hybrid cloud/edge and IoT systems has to address (MUST/MAY) as follows.

- **(R1) Scalability**: it MUST implement a scalable assurance process, quickly adapting to the size and complexity of the target system.
- **(R2) Distributed**: it MUST adopt a distributed architecture based on a hybrid cloud/edge deployment.
- **(R3) Flexibility**: it MUST support parameterized evaluation according to the target system, with flexible scheduling policies (e.g., repeated, one shot) [11].
- **(R4) 5G-readiness**: it MUST support the interaction with devices over mobile networks, in particular 5G, which is one of the IoT-enabling technologies [12].
- **(R5) Deployability**: it MUST provide automated (edge) deployment of its components, accommodating different scenarios such as public, on-premises, hybrid.
- **(R6) Stateful analysis**. It MUST implement techniques analyzing the historical evolution of the whole system.
- **(R7) Integration**. It MAY allow easy integration with other security systems, enabling patterns such as promptly reaction to detected non-compliances.

To the best of our knowledge, no framework addresses the above requirements offering a scalable, flexible, and fully distributed solution for edge and IoT assurance.

III. Framework Architecture

The main pillar of our framework is the cloud/edge paradigm, corresponding to *i)* a cloud layer where assurance results, coming from the below layer, are aggregated, evaluated, and stored creating a holistic view of the target system; *ii)* an edge layer where assurance evidence, collected at the perception layer from IoT devices, is preprocessed according to an initial analysis.

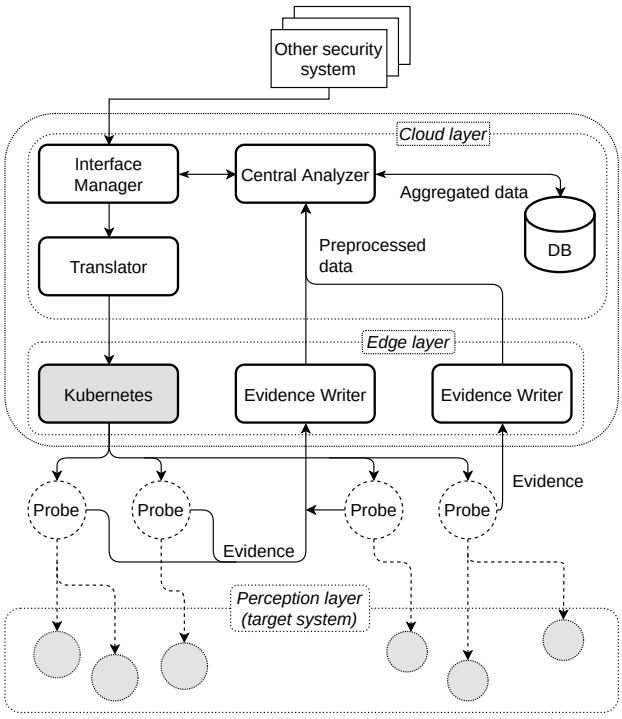

Figure 1. Architecture of the proposed framework.

The framework in Figure 1 has Kubernetes as its core technology, enabling out of the box horizontal scalability, high availability, and support for edge computing and 5G [13]. The framework consists of a set of microservices operating both on the cloud and on the edge, as follows.

- **Interface Manager** exposes a REST interface to programmatically manage all the functionalities of the framework. It runs on cloud, and governs at high-level the assurance process by communicating with *Translator*.
- **Translator** ties up cloud and edge layer, exposing a REST interface that translates assurance requests into low-level Kubernetes requests; they are then sent to Kubernetes, that takes care of *probes* scheduling and execution.
- **Probes** are self-contained scripts for evidence collection. They are natively executed on edge by Kubernetes, and return as output *i)* a Boolean result indicating the success (*true*) or the failure (*false*) of the assurance evaluation; *ii)* additional low-level evaluation details.
- **Evidence Writer** collects and preprocesses *probes* results on edge, by cleaning, filtering, and temporally aligning them.
- **Central Analyzer** receives the preprocessed data from *Evidence Writer*, aggregates and evaluates them to create a holistic view of the target system, according to the target devices position and past history.

The cloud/edge framework addresses (R2) and (R4), and the clean separation of concerns among the components combined

with Kubernetes provides support for (R1) and (R5). *Probes* enable (R3), as all the low-level details required to collect evidence from IoT devices are self-contained within each *probe*. *Evidence Writer* and *Central Analyzer* partially address (R6), being responsible for assurance results alignment and complex analysis. The REST interface exposed by *Interface Manager* allows the integration of other components exploiting the framework functionalities, providing the basis for (R7). In general, the framework can easily assess traditional IT systems (e.g., cloud), as well as new generation hybrid cloud/edge/IoT systems communicating over heterogeneous technologies (e.g., 5G, WiFi). Finally, the presented framework takes advantage of the cloud/edge paradigm, shaping a new direction for security assurance in edge and IoT systems. It is a complete redesign of traditional frameworks, fitting most application scenarios and effectively demonstrating security properties, regardless of the complexity of the target system.

IV. Framework in a Use Case

We present a real-world application of our framework in a Medical Things (IoMT) scenario. We consider a large and modern hospital incorporating all the challenges in Section II-A [14]. It includes a significant amount of heterogeneous devices, from simple sensors (e.g., for temperature and humidity), to smart 5G IoMT devices for surgery and patient monitoring. Guaranteeing the correct system behavior is critical, as malfunctions can seriously threat patients lives. First, the hospital must have all the devices under control. Traditional solutions are not effective in this respect, as they cannot be smoothly migrated from conventional scenarios to complex IoT environments without undermining their effectiveness. In particular, they fail to catch on typical behaviors of IoT devices, for instance, being offline for short periods (i.e., not responding but working). The extent and the distribution of the whole hospital system is also challenging, requiring a deep architectural redesign, and making the use of traditional assurance solutions not suitable. Finally, it is crucial that collected data reflect how the system is really working, with particular attention to the trustworthiness of such data.

In other words, traditional assurance techniques are not applicable in this scenario. Instead, the proposed framework in Section III is well-suited. It performs assurance evaluations grounded on evidence collected in a lightweight manner directly on the field, according to fine-grained scheduling requirements. This collection process, implemented by *probes*, scales horizontally with the size of the IoMT environment. It can accommodate heterogeneous target devices, as low-level networking details are confined at *probe*-level. Furthermore, the framework can process the large amount of evidence produced by all the *probes*. *Evidence Writer* scales horizontally, preprocessing evidence with low-latency before a final aggregation and storage by *Central Analyzer*.

In other words, the proposed framework overtakes conventional security assurance systems enabling an approach that otherwise would be challenging. A traditional assurance deployment would combine different control systems for each organization unit with hybrid security solutions, that soon would break out in an uncontrollable scenario. In contrast, our solution provides an easily manageable and highly automated framework. Altogether, it enables to obtain a holistic view of the target system, considering the single devices, the zones where they are located, the relationships among them, and, finally, the system as a whole.

V. Conclusions

Having confidence that an IT system behaves as expected is fundamental in any scenario, but is critical in modern distributed systems, where the confluence of multiple computing paradigms results in systems difficult to control and assess. Traditional assurance methodologies must then be redesigned towards more flexible and adaptive approaches. In this paper, we envision a security assurance framework for edge and IoT systems based on a distributed cloud/edge architecture backed by Kubernetes. Our work represents a transition point from existing security assurance frameworks to more modern solutions. This leaves space for aspects to be faced going forward, such as a thorough experimental evaluation on an real-world scenario, and an effective stateful analysis exploiting machine learning techniques.

References

[1] Cisco. (2020) Cisco Annual Internet Report (2018–2023) White Paper.

[2] J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, and A. Marrs, *Disruptive technologies: Advances that will transform life, business, and the global economy*. McKinsey Global Institute San Francisco, CA, USA, 2013.

[3] C. Ardagna, R. Asal, E. Damiani, and Q. Vu, "From Security to Assurance in the Cloud: A Survey," *ACM Computing Surveys*, vol. 48, no. 1, August 2015.

[4] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," *IEEE IoT-J*, vol. 5, no. 4, Aug. 2018.

[5] M. Aslam, B. Mohsin, A. Nasir, and S. Raza, "FoNAC - An automated Fog Node Audit and Certification scheme," *Computers & Security*, vol. 93, June 2020.

[6] M. Anisetti., C. Ardagna., N. Bena., and E. Damiani., "Stay Thrifty, Stay Secure: A VPN-based Assurance Framework for Hybrid Systems," in *Proc. of SECRYPT 2020*, Paris, France, July 2020.

[7] T. Ahanger and A. Aljumah, "Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms," *IEEE Access*, vol. 7, 2019.

[8] D. Rani and N. S. Gill, "Review of various iot standards and communication protocols," *Int. J. Eng. Res. Technol*, vol. 12, no. 5, 2019.

[9] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge Computing Security: State of the Art and Challenges," *Proceedings of the IEEE*, vol. 107, no. 8, Aug. 2019.

[10] P. Pantazopoulos, S. Haddad, C. Lambrinoudakis, C. Kalloniatis, K. Maliatsos, A. Kanatas, A. Varádi, M. Gay, and A. Amditis, "Towards a Security Assurance Framework for Connected Vehicles," in *Proc. of IEEE WoWMoM 2018*, Chania, Greece, June 2018.

[11] A. Hamza, H. H. Gharakheili, and V. Sivaraman, "IoT Network Security: Requirements, Threats, and Countermeasures," *arXiv:2008.09339 [cs]*, Aug. 2020.

[12] J. M. Khurpade, D. Rao, and P. D. Sanghavi, "A Survey on IOT and 5G Network," in *Proc. of ICSCET 2018*, Mumbai, India, Jan. 2018.

[13] H. Fathoni, C.-T. Yang, C.-H. Chang, and C.-Y. Huang, "Performance Comparison of Lightweight Kubernetes in Edge Devices," in *Proc. of I-SPAN 2019*, Naples, Italy, 2019.

[14] B. Cheng, M. Wang, S. Zhao, Z. Zhai, D. Zhu, and J. Chen, "Situation-Aware Dynamic Service Coordination in an IoT Environment," *IEEE/ACM Transactions on Networking*, vol. 25, no. 4, Aug. 2017.