BRAIN-IoT Architecture and Platform for Building IoT Systems

Salim Chehida[1][a], Saddek Bensalem[1][b], Davide Conzon[2][c], Enrico Ferrera[2][d] and Xu Tao[3]
[1] *CNRS, VERIMAG, University of Grenoble Alpes, Grenoble, France*
[2] *IoT and Robotics Area, LINKS Foundation, Turin, Italy*
[3] *Computer Science Department, University of Kentucky, U.S.A.*

Keywords: IoT, Architecture, Model-based Design, Interoperability, Distributed Execution, Security and Privacy, Monitoring, Resiliency, Cloud, Edge, Decentralized IoT Applications.

Abstract: The integration of Internet of Things (IoT) for building complex and critical systems requires powerful platforms enabling to deal with multiple issues, including modeling, monitoring, control, maintaining and management of IoT applications. In this work, the authors propose a new platform based on layered architecture that integrates a set of assets for model-based development of IoT systems. This platform named BRAIN-IoT aims to meet the new challenges of IoT applications and to reduce the effort for building and managing these applications. It consists of three frameworks that allow building decentralized IoT applications with computing capacity at the edge in a computing continuum with the cloud. The modeling and validation framework is used to design, develop, and validate IoT applications logic. The distributed execution framework provides an autonomic distributed infrastructure for the dynamic deployment and execution of IoT services on a mixed cloud-edge environment. The security framework enables access control, end-to-end security and privacy of data collected using IoT devices. The BRAIN-IoT platform is mapped to a well-established IoT reference architecture and experimented on two industrial use cases.

1 INTRODUCTION

In recent years, IoT has demonstrated to be able to offer significant improvements to various domains, e.g., health, energy, hydraulics, and transport. Several architectures and platforms (Adolphs and Epple, 2015; Lin et al., 2019; Römer et al., 2020; Bauer et al., 2013; IEEE, 2020) have been proposed for building IoT systems. However, the complexity and the dynamic of these systems highlights the need for new solutions that allow promoting automation, managing complexity and increasing trust. To cope with these demanding requirements, a multitude of novel technologies such as Edge Computing, Artificial Intelligence (AI), and Analytics, as well as Security, Privacy and Trust schemes are being investigated to be adopted in current IoT architectures standards.

The 3D IoT architecture (Vermesan and Bacquet, 2018) specified by Alliance for the Internet of Things Innovation (AIOTI) (AIOTI, 2020) is high-level architecture proposed for supporting the novel requirements that generic IoT applications have. It aims to be one pioneer of the next-generation IoT paradigm, establishing a novel generic reference for different IoT/Industrial Internet of Things (IIoT) applications from different domains. In this work, the authors present a new platform founded on a layered concrete architecture based on the 3D reference model. The BRAIN-IoT platform integrates novel technologies to address the following challenges that arise in recent IoT applications:

C1) Facilitate IoT systems modeling through multiple abstractions and enabling the integration of Validation and Verification (V&V) techniques and tools.

C2) Enable designing IoT applications involving several heterogeneous platforms and Smart Things interconnected to each other in a distributed environment.

C3) Support the analysis and exploitation of large amount of raw data to extract and predict information supporting system automaticity and autonomicity.

[a] https://orcid.org/0000-0002-5070-2591
[b] https://orcid.org/0000-0002-5753-2126
[c] https://orcid.org/0000-0002-2962-8702
[d] https://orcid.org/0000-0002-4671-3861

Chehida, S., Bensalem, S., Conzon, D., Ferrera, E. and Tao, X.
BRAIN-IoT Architecture and Platform for Building IoT Systems.
DOI: 10.5220/0011086000003194
In *Proceedings of the 7th International Conference on Internet of Things, Big Data and Security (IoTBDS 2022)*, pages 67-77
ISBN: 978-989-758-564-7; ISSN: 2184-4976

C4) Ensure the deployment of services in a distributed environment, dynamic resources allocation in response to environmental changes, and autonomous dependency management to reduce the system operational complexity.

C5) Ensure the security, privacy, and resiliency in resource-constraint and distributed IoT environments.

In this work, the authors validate the BRAIN-IoT platform through two use cases for warehouse logistics and for water distribution management. The solution is evaluated using a standard well-known usability questionnaire, the User Experience Questionnaire (UEQ)[1], which allows the end-users to evaluate their feeling with the product in question.

Section 2 presents the existing IoT architectures and platforms. Section 3 and 4 show the BRAIN-IoT Architecture and its integrated components. In Section 5, the authors map BRAIN-IoT components with the 3D IoT reference architecture. Section 6 presents the applications leveraged to validate the architecture. Section 7 briefly explains the validation results. Finally, the authors draw conclusions in Section 8.

2 RELATED WORK

Nowadays, it is still not available an unique IoT reference architecture. Several different organizations and consortia have tried to define it, but the scenario is still fragmented. This section presents the available IoT reference architectures, describing their main characteristics.

The Reference Architecture Model Industrie 4.0 (RAMI 4.0) (Adolphs and Epple, 2015) is a reference architecture focused on the smart industry domain. The effort has been started in Germany, but today is driven by several companies and foundations in relevant industry sectors, i.e., the ones associated in the Platform Industrie 4.0[2]. RAMI 4.0 is a Service Oriented Architecture (SOA), which combines all elements and Information technology (IT) components in a layered and life cycle model. RAMI 4.0 breaks down complex processes into easy-to-grasp packages, including data privacy and IT security. Since the architecture is focused on the industry domain, it does not cover the requirements of generic IoT applications.

The Industrial Internet Reference Architecture (IIRA) (Lin et al., 2019) is a common architecture framework defined by the Industry Internet of Things Consortium (IIC), to develop interoperable IIoT systems for applications across a broad spectrum of industrial verticals, both public and private, to achieve the IIoT goals. Also in this case, the architecture is interesting, but it is focused only on industrial domain, so it is not suitable to be applied in a more generic IoT scenarios.

The Eclipse Arroehead (Römer et al., 2020) is a SOA with a reference implementation for IoT interoperability that was originally developed as part of the Arrowhead Tools European research project[3], aligned with the concept of RAMI 4.0 and IIRA. Also in this case, the architecture is mainly focused on industry 4.0 applications, but it can be also adapted to smart cities, e-mobility, energy, and buildings domains.

The Internet of Things Architecture (IoT-A) (Bauer et al., 2013) is a reference architecture for IoT applications, which has been defined as an outcome of the IoT-A European Union (EU) project[4], which had the main objective to develop an architectural reference model for the interoperability of IoT systems. The last version of the architecture has been defined in 2013 at the end of the project, but its use as reference model is currently limited.

The Standard for an Architectural Framework for the Internet of Things (IoT) (IEEE, 2020) has defined an architecture framework description for IoT, which conforms to the international standard International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)/Institute of Electrical and Electronics Engineers (IEEE) 42010:2011. The standard provides an architectural blueprint for Smart City implementation, considering cross-domain interaction and enabling semantic interoperability among various domains and components of a Smart City (e.g., mobility, healthcare). For this reason, also if not specialized for a single domain, the standard is limited to Smart City related applications.

The results of the newest research projects, especially in the EU, brought to the harmonization of several standard approaches, which brought to the 3D IoT Architecture model(Vermesan and Bacquet, 2018) as shown in Figure 1. The AIOTI High Level Architecture (HLA) (AIOTI, 2020) has been defined by the AIOTI Working Group (WG) Standardization for IoT to be applied by Large Scale Pilots (LSPs) projects[5]. Capturing the commonalities shared among Reference Architectures of the LSPs, the 3D Reference Architecture has been produced from the EU

[1] https://www.ueq-online.org/

[2] https://www.plattform-i40.de/IP/Navigation/DE/Home/home.html

[3] https://www.eclipse.org/org/research/project/

[4] https://cordis.europa.eu/project/id/257521/it

[5] https://european-iot-pilots.eu/

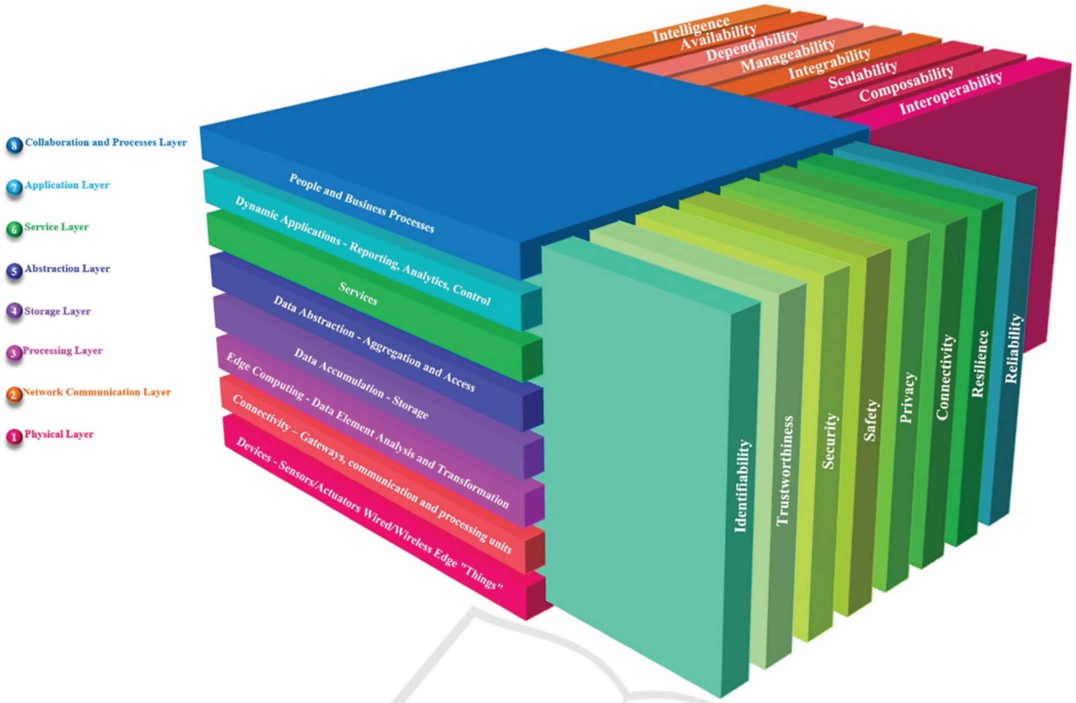
8 Collaboration and Processes Layer
7 Application Layer
6 Service Layer
5 Abstraction Layer
4 Storage Layer
3 Processing Layer
2 Network Communication Layer
1 Physical Layer
People and Business Processes
Dynamic Applications - Reporting, Analytics, Control
Services
Data Abstraction - Aggregation and Access
Data Accumulation - Storage
Edge Computing - Data Element Analysis and Transformation
Connectivity – Gateways, communication and processing units
Devices - Sensors/Actuators Wired/Wireless Edge "Things"
Intelligence
Availability
Dependability
Manageability
Integrability
Scalability
Composability
Interoperability
Identifiability
Trustworthiness
Security
Safety
Privacy
Connectivity
Resilience
Reliability

Figure 1: 3D IoT architecture (Vermesan and Bacquet, 2018).

project CREATE-IoT[6]. The 3D architecture is generic and offers a representation that can include the different IoT/IIoT applications across different sector domains (e.g., automated/autonomous vehicles, smart farming, smart cities, energy, manufacturing, health). The architecture includes the function by design concept with end-to-end functions addressed across the 8 layers. This allows addressing the heterogeneous applications including different IoT platforms and processing at the edge, fog, and cloud. The LSPs projects are reflecting such a model in their architectures, which completely represents this new level of complexity.

In this work, we present a new concrete architecture platform based on the 3D model. The BRAIN-IoT platform is developed in an EU project[7]. It provides a set of integrated assets to build IoT applications from different domains. Assets can be used in the different stages of the IoT development process, starting from modeling to deployment and maintenance. They provide the key functions defined by the 3D reference model to address next-generation IoT challenges. The next two sections will introduce the BRAIN-IoT architecture, which then will be mapped in the 3D reference model.

3 BRAIN-IoT ARCHITECTURE

Figure 2 shows the BRAIN-IoT architecture, which includes several assets structured in six layers.

The *application layer* describes the applications that are built. As mentioned earlier, the BRAIN-IoT platform can be applied for generic IoT applications. In this work, two scenarios will be presented : Service Robotics for Warehouse Logistics (SRWL) and Critical Infrastructure for Water Distribution Management (CIWDM). SRWL is a special logistic service involving several robotic platforms from Robotnik Automation company[8], which need to collaborate to scan a given warehouse and to assist humans in a logistic domain. A fleet of robots supports the movement of different loads in a warehouse. CIWDM is a scenario related to the management of water distribution network in collaboration with EMALCSA company[9]. It focuses on monitoring and control the management of the water urban cycle in metropolitan environment of the city of la Coruna in Spain. More details on the applications realized by the BRAIN-IoT platform are described in Section 6.

The *modeling and validation layer* provides several functions, e.g., design of complex IoT systems considering several abstraction levels, simulation and

[6] https://european-iot-pilots.eu/project/create-iot/

[7] https://www.brain-iot.eu/

[8] https://robotnik.eu/

[9] https://www.emalcsa.es/index.php/es/

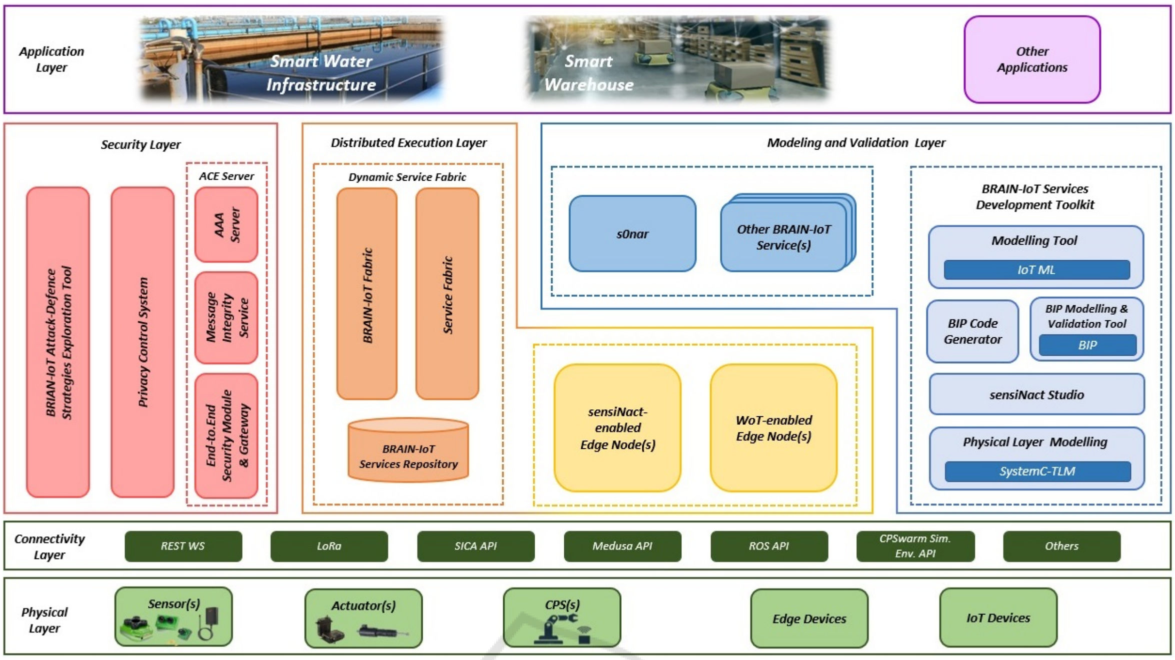

Figure 2: BRAIN-IoT architecture.

validation of systems behavior before their real deployment, automatic code generation from the models, ensuring online intelligent services for prediction and anomaly detection based on data, monitoring and controlling IoT applications, modeling IoT devices and checking the correctness of systems before its deployment in the physical world.

The *distributed execution layer* is responsible of dynamic deployment and execution of IoT applications. It allows assembling, configuring and maintaining runtime applications. It contains required IoT services as well as functionalities for discovery, look-up, and name resolution of IoT services. This layer is also responsible for operational management and monitoring of specific devices via the gateways deployed to each BRAIN-IoT Edge Node.

The *security layer* provides multiple services for protecting IoT systems such as security risk assessment of IoT systems (Chehida et al., 2021), ensuring end-to-end security from IoT devices/Cyber Physical System (CPS) to application (Maillet-Contoz et al., 2020), ensuring identity and distributed access control management for IoT devices/CPS and users, and the implementation of privacy features for the IoT applications (Rashid et al., 2019).

The bottom layers represent *connectivity protocols* and *Application Programming Interface (API)* such as Long Range (LoRa) and Robot Operating System (ROS), and physical IoT devices, e.g., actuators, sensors.

4 BRAIN-IoT INTEGRATED PLATFORM

Figure 3 shows the BRAIN-IoT integrated assets available in the Eclipse Research Lab[10], which responds to challenges C1, C2, C3, C4 and C5 presented in Section 1.

The *BRAIN-IoT Services Development Toolkit* adopts a methodology and toolset for modeling different abstraction levels of IoT systems (C1). It is responsible for designing the logic of the IoT Application, which composes the services provided by available devices (i.e., sensors, actuators, CPSs) and external services (e.g., weather forecast, open data, third-party IoT platforms, databases) based on their interactions. The application logic is modelled along with the relevant IoT environment using IoT-ML through *BRAIN-IoT Modeling Tool*. The *IoT-ML Modeling Tool* defines a Domain-Specific Modelling Language (DSL), based on Unified Modeling Language (UML) (UML2, 2017), to describe system-level components choices and their dependencies, also IoT devices capabilities. Then, the IoT-ML model is refined to Behavior, Interaction, and Priority (BIP) model representing formally the components behavior and their possible interactions using automata-based models expressed in the BIP language (Basu et al., 2011). The BIP language integrated in BRAIN-IoT platform

[10] https://github.com/eclipse-researchlabs/brain-iot

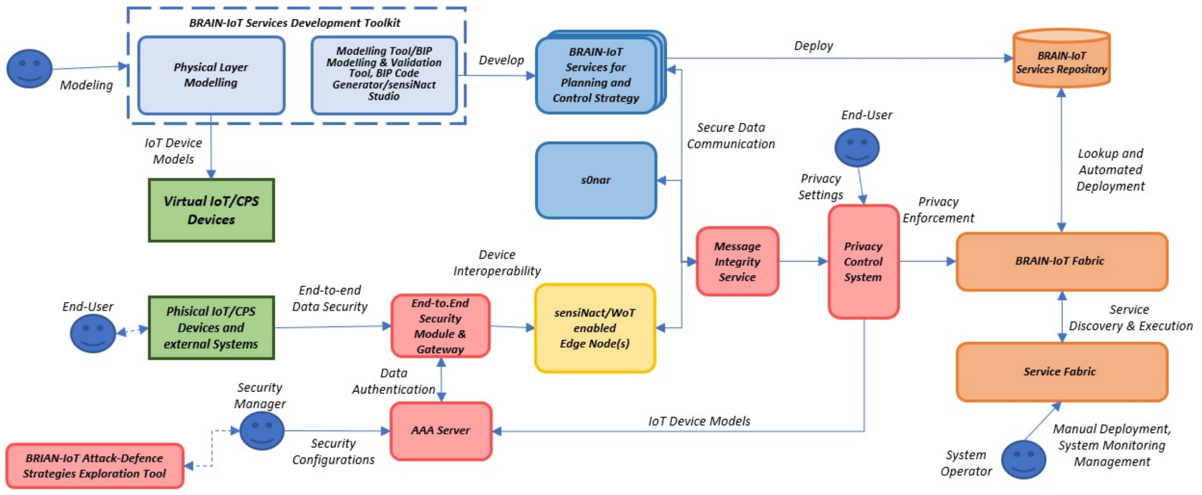
BRAIN-IoT Services Development Toolkit
Modeling
Physical Layer Modelling
Modelling Tool/BIP Modelling & Validation Tool, BIP Code Generator/sensiNact Studio
Develop
BRAIN-IoT Services for Planning and Control Strategy
Deploy
BRAIN-IoT Services Repository
IoT Device Models
Virtual IoT/CPS Devices
sOnar
Secure Data Communication
End-User
Privacy Settings
Privacy Enforcement
Lookup and Automated Deployment
Message Integrity Service
Privacy Control System
BRAIN-IoT Fabric
Device Interoperability
End-User
Physical IoT/CPS Devices and external Systems
End-to-end Data Security
End-to.End Security Module & Gateway
sensiNact/WoT enabled Edge Node(s)
Service Discovery & Execution
Service Fabric
Data Authentication
Security Manager
AAA Server
IoT Device Models
BRIAN-IoT Attack-Defence Strategies Exploration Tool
Security Configurations
Manual Deployment, System Monitoring Management
System Operator

Figure 3: BRAIN-IoT Integrated Assets.

gives a precise semantics to the system models expressed by IoT-ML. Also, the *BIP Modelling and Verification Tool* provides efficient tool for verification and analysis of the BIP models based on Statistical Model Checking (SMC) technique. SMC uses simulation-based approach to reason about formal requirements expressed in temporal logic properties. After simulation and verification, the BIP model is converted in Java source code as application artefacts through the *BIP Code Generator*. The generated artifacts are then released and stored in *BRAIN-IoT Services Repository*, to be deployed and executed by the distributed execution framework. The BRAIN-IoT modeling and validation framework also offers the ability to use development-time models to supervise running execution platform states using *sensiNact Studio*. This solution enables monitoring of BRAIN-IoT services and starting or stopping them from the *BRAIN-IoT Services Development Toolkit*. In addition, the generated IoT applications, named as BRAIN-IoT services, can be validated leveraging IoT physical device models with *Physical Layer Modelling Tool* based on SystemC-TLM language (Ghenassia, 2006) to validate the correctness of the system behavior, before deploying it in the physical world. Thanks to the Physical Layer Modelling Tool, the system reliability is increased, as the validation strategy of the end-device is strengthened by adding scenarios focusing on device robustness considering its interaction with system environment. Nevertheless, at the system level modelling, it is able to describe the services provided by the existing IoT devices with Web of Things (WoT) Thing Description[11], so that enforces the services composition in the system models and provides the inputs to the edge node at runtime to communicate with the external IoT device using the communication protocol it supports. Finally, an AI approach supported by the *sOnar tool* is provided to model and implement AI modules, which can be composed with the system behavior models (C3). The sOnar tool provides the online data analysis service for anomaly detection and prediction functionality using machine learning techniques. It acts as an intelligent computing unit to enable autonomic functionalities for the Runtime Infrastructure through the deployment and execution of reusable software AI/ML algorithms. It sends notifications to the execution framework to trigger a prompt reaction that mitigates or avoids negative consequences to the IoT/CPS systems.

The BRAIN-IoT distributed execution framework provides an autonomic distributed infrastructure (*BRAIN-IoT Fabric*) for the dynamic deployment, discovery and execution of BRAIN-IoT services on a mixed cloud-edge environment (C4). The BRAIN-IoT Fabric is combined with the *Paremus Service Fabric* to manage communications between the developed applications from *BRAIN-IoT Services Repository* through asynchronous events using the BRAIN-IoT EventBus. By using BRAIN-IoT EventBus, the multiple deployed applications are completely decoupled and the failure of one application has no impact on other running applications. The distributed execution framework also provides the interoperability for the external IoT devices/platforms, using *WoT-enabled Edge Nodes* based on a World Wide Web Consortium (W3C) WoT Thing Description of the communications interface and *sensiNact Edge Nodes* (Gürgen et al., 2016) based on Eclipse sensiNact gate-

[11] https://www.w3.org/TR/wot-thing-description/

way[12], which can be deployed in a distributed and bulk manner (C2). The sensiNact-enabled Edge Node provides connectivity, interoperability, and data processing to various IoT devices by its capability to interact with a wide variety of equipment and protocols, as well as its extensibility mechanisms. The WoT-enabled Edge Node implements an approach to enable the interoperability between ROS-based CPS applications and other heterogeneous IoT platforms in a sophisticated IoT software ecosystem.

The BRAIN-IoT security framework provides a *Security Module and Gateway*, a *Message Integrity Service (MIS)*, and a distributed *Authentication, Authorization, and Accounting (AAA) Server* to ensure data confidentiality, integrity, availability, and authentication for the BRAIN-IoT platform (C5). The security module authenticates and encrypts data sent over the network at the application level with reduced energy consumption for IoT sensors and actuators. The security gateway checks the sender's authentication before decrypting the data. The distributed AAA server manages identity and rights from users and IoT devices. The MIS signs the data event before sending it and verifies the message integrity and sender authentication when the event is received by a node. The *Attack-Defense Strategies Exploration Tool* (Chehida et al., 2020) is a decision-supporting tool which gives the suggestions for the security considerations by providing insightful information that allows the security manager to evaluate system vulnerabilities and to design reliable security policies. The tool identifies the potential attack actions that are most likely to succeed such as network attacks and data manipulation known as False Data Injection Attacks (FDIAs). It also selects high impactful defense actions that make the system harder to attack while finding a balance between the attack cost and its probability of success. Furthermore, the *Privacy Control System* provides the policy-based mechanism for the IoT users to protect the personal data collected using IoT devices. It is based on a Policy Enforcement Point (PEP) that applies the policies and controls access to the data by available services. It attaches the policies to the data event and delivers it along with the data over the EventBus. The Privacy Control System aims allowing a Privacy-as-a-Service approach and facilitating the adoption of privacy policies control in IoT environments based on SOA.

5 MAPPING BRAIN-IoT ASSETS WITHIN THE 3D MODEL

The BRAIN-IoT architecture previously presented is based on the 3D architecture introduced by AIOTI. To better explain the link between the two architectures, this section presents the mapping of the BRAIN-IoT main components in the 3D architecture as shown in Figure 4.

Specifically, the *Physical layer* includes actuators, sensors and CPSs providing the connectivity cross-cutting function and useful to support integrability. On the *Network Connectivity Layer* there are the End-to-end Security Module and Gateway providing security and integrability as well as a set of different APIs providing connectivity and integrability. On the *Processing Layer* there are the Privacy Control System for privacy control and dependability, as well as the sensiNact Edge Nodes and the WoT Enabled Edge nodes that provide connectibity and interoperability; at the same layer the AAA server and the MIS providing reliability and dependability. The *Storage Layer* includes the BRAIN-IoT Services Repository providing resilience and availability. On the *Service Layer* there are BRAIN-IoT Fabric that provides connectivity and composability; the BRAIN-IoT Moelling Tool to provide manageability; the IoT-ML that provides interoperability; the BIP Code Generator, which provides dependability; sOnar providing intelligence; Brain-IoT Physical Layer Modeling Language to provide connectivity and integrability. Finally on the *Application Layer* there are the BRAIN-IoT Attack-Defense Strategies Exploration Tool providing security and availability as well as the sensiNact Studio that provides connectivity and manageability.

This mapping shows that the BRAIN-IoT components are able to provide the main IoT cross-cutting functions and IoT system properties needed to satisfy the requirements of next-generation IoT challenges.

6 APPLICATIONS

As said in Section 3, the BRAIN-IoT platform has been validated through two main scenarios: Service Robotics for Warehouse Logistics (SRWL) and Critical Infrastructure for Water Distribution Management (CIWDM).

In the first scenario, the BRAIN-IoT platform supported the implementation of a multi-agent system for the distributed self-organized management of a fleet of robots to move loads among the different areas of a warehouse. The movement of these loads does not require any operator to control the fleet. Robots are

[12] https://projects.eclipse.org/projects/technology.sensinact

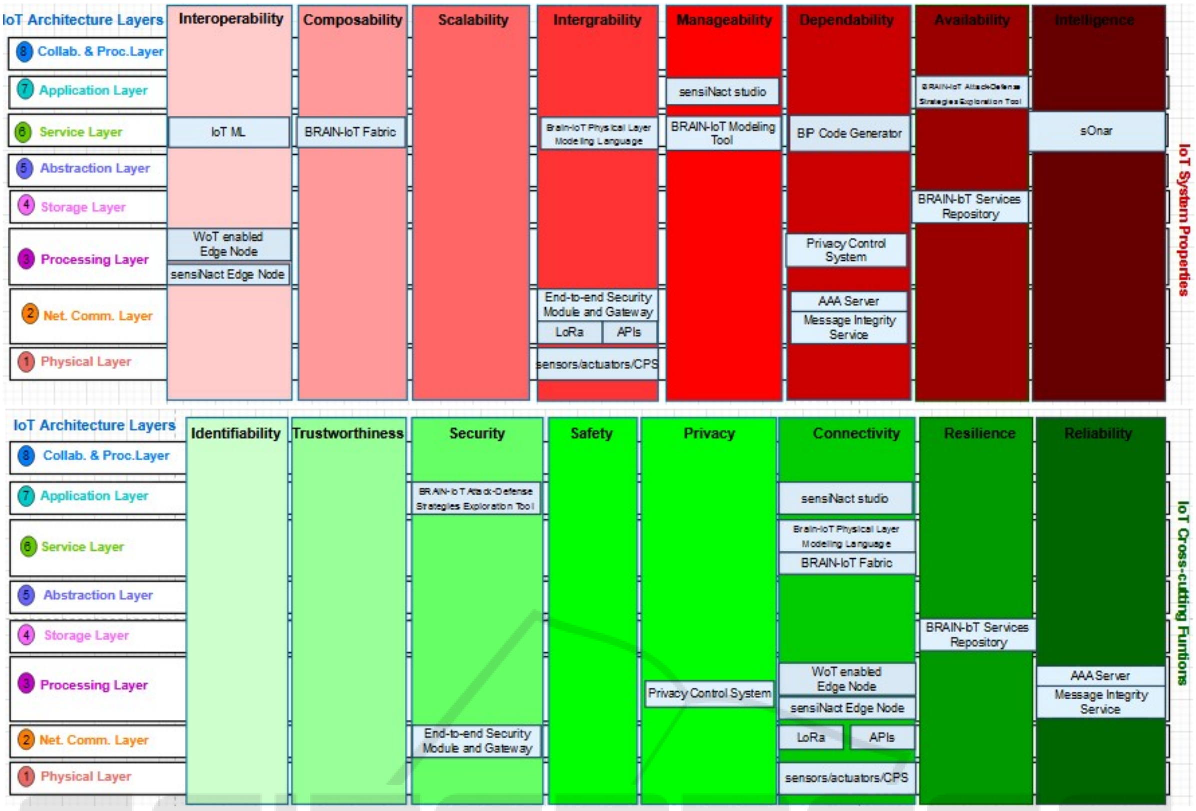

Figure 4: Mapping BRAIN-IoT assets with 3D IoT architecture.

expected to empty continuously the “inbound area” of the warehouse, where the loads are temporarily positioned when items are delivered in for storage, moving them to a specific place in the ”storage area”. When triggered by the human operator, each robot autonomously moves from their base station to the inbound area and patrols looking for the loads and identifying them through their barcode. Consequently, the robot establishes a communication with the backend system of the warehouse to ask which cell of the ”storage area” the load must be placed in. When the backend system return back the coordinates of the storage cell, the robot picks the load up and moves it through the warehouse to the right position in the storage area. The navigation of the robots across the warehouse is designed to be safe, avoiding obstacles along the path, and adaptable to the specific environment where the fleet of robots is deployed. For instance, the same warehouse logistics application has been deployed in a scenario similar to a supermarket, where the items to store can also be perishable, e.g. like fruits and vegetables or fish and meat. In such scenario, the storage area must be kept at a specific environment temperature to not ruin the food, and it is separated from the the other warehouse areas by a controllable door. In such scenario, the robots are able to discover the door as a new controllable service available on the network. Consequently, through the BRAIN-IoT platform it is able to trigger the deployment at run time of a new driver which enables the interaction with the automated door. Afterwards, the robots capabilities are then augmented allowing them to navigate across the warehouse also opening and closing the door when needed. In this scenario, the main objectives of the application of the BRAIN-IoT platform were to reduce the development time for multi-agent robot applications, establishing a secure end-to-end interaction with robotic platforms (more specifically ROS-based[13] robots) as well as legacy backend systems and external devices within the surrounding environment. Moreover, the use-case allowed also to demonstrate and evaluate the dynamic autonomous reconfiguration of the system for self-adaptation to the environment layout and anomaly situations.

In the second scenario, the BRAIN-IoT platform is adopted to implement a safe autonomous control for the management of a critical infrastructure like the one distributing the water in the city of A Coruña, in Spain. The objective is to collect and exploit data coming from geographically distributed and hetero-

[13] https://www.ros.org/

geneous devices and platforms, used for water level monitoring and treatment, with the aim of early detecting abnormal and critical situations that may hinder the correct functioning of the infrastructure or even damage it. The good quality of the data is fundamental for creating accurate indicators for decision making and for real-time adaptive control procedures. For this reason, the protection of the numerous resource-constrained sensors and meters is extremely important to guarantee the dependability of the measured data. Also, it is very important to guarantee that all the different data sources are authorized to provide data, and no malicious injection of fake information are present. More specifically, the needed control consists in the following: when the level of water reaches a specific threshold, the spillgates shall be opened. Normally, the spillgates opening is manually performed. In this use case, BRAIN-IoT platform controls automatically the spillgates opening, based on the measures of the water flows. Such control strategies are modelled and developed with the BRAIN-IoT Modelling Tool. A model-based approach allows to modify in an agile way the control strategies whenever, in the future, modifications or improvements will be needed. Furthermore, the BRAIN-IoT platform is used for collecting data from different water flow meters placed in different locations and analyzing them to detect possible deviations w.r.t. the normal behaviour. In fact, possible data outliers (e.g. due to device obsolescence, miscalibration, external attacks) may be extremely risky for the water infrastructure because data are used to control the spillgates for let the water flowing correctly in the pipes and deliver the water correctly to the customers. According to the outcomes of the analysis, the BRAIN-IoT platform must autonomously reconfigure the spillgates control strategy in such a way to cut off the ones which are directly affected by the meter's misbehaviors. This approach allows to: enhance the resiliency of the water infrastructure from failures in order to provide a service which has reduced possibilities of discontinuity; identify in real-time the possible problems with the meters and sensors, allowing a prompt reaction for mitigating the issues and provide a better service experience to the customers; collect as a whole the data coming from heterogeneous meters and sensors which are spread all over the city.

7 VALIDATION RESULTS

The BRAIN-IoT platform has been evaluated through workshops conducted carrying out a usability assessment performing several teleconferences with relevant stakeholders and were oriented to the compilation of a standard well-known usability questionnaire, which allows end-user of a product to evaluate their feeling with the product in question. The results of the inquiry demonstrated to be very valuable to measure the interest from the stakeholders for the provided functionalities and their degree of satisfaction with the overall BRAIN-IoT Platform.

Using the UEQ, the items are scaled from -3 to +3, where -3 represents the most negative answer, 0 a neutral answer, and +3 the most positive answer. The items are categorised into six dimensions each of which consists of 4-6 items on the UEQ which thus describes a distinct quality aspect of an interactive product. *Attractiveness*: general impression towards the product. *Efficiency*: is it possible to use the product fast and efficient? *Perspicuity*: is it easy to understand how to use the product? *Dependability*: does the user feel in control of the interaction? *Stimulation*: is it interesting and exciting to use the product? *Novelty*: Is the design of the product innovative and creative? The results are also evaluated using a benchmark. For this analysis, the measured scale means are set in relation to existing values from a benchmark data set, which contains data from 20190 persons from 452 studies concerning different products (business software, web pages, web shops, social networks). The benchmark classifies a product into 5 categories (per scale). *Excellent*: in the range of the 10% best results. *Good*: 10% of the results in the benchmark data set are better and 75% of the results are worse. *Above average*: 25% of the results in the benchmark are better than the result for the evaluated product, 50% of the results are worse. *Below average*: 50% of the results in the benchmark are better than the result for the evaluated product, 25% of the results are worse. *Bad*: in the range of the 25% worst results.

The results of the evaluation of the BRAIN-IoT platform show that the stakeholders perceived it as an innovative solution. The discussion during the workshops let the self-administrative capabilities emerged as the main innovative functionality, along with the capacity of distribute edge intelligence in a decentralized environment. The good score for the dependability of the platform is due to the good comments about the security perspective, more specifically for the capability of protecting data sourced by resource constrained devices, as well as the capacity to provide the data owner the control of the access policies of their data. Despite one of the objectives of BRAIN-IoT is to relief the IoT developers and system operators from the burden of implementing and operating IoT applications involving multiple hetero-

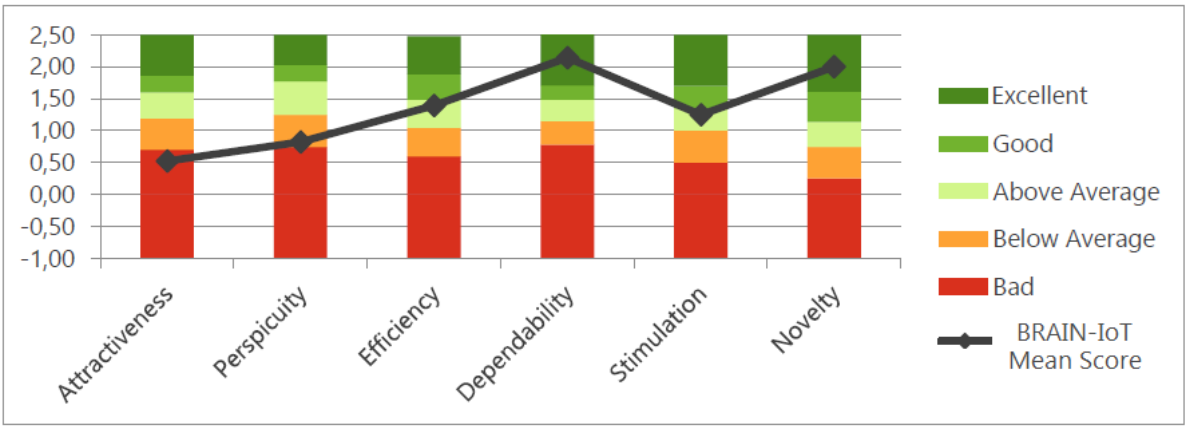

Figure 5: Validation results of the BRAIN-IoT platform.

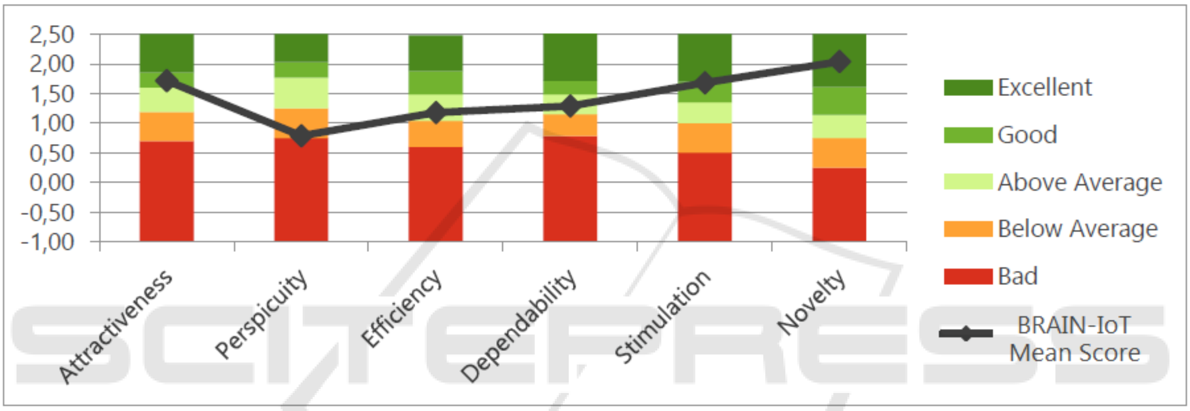

Figure 6: Validation results of the BRAIN-IoT platform applied to the SRWL scenario.

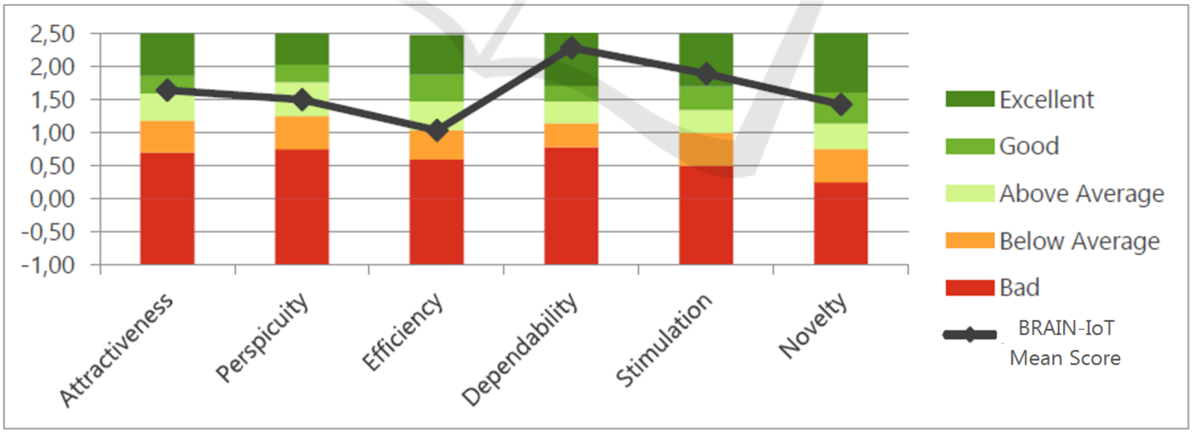

Figure 7: Validation results of the BRAIN-IoT platform applied to the CIWDM scenario.

geneous existing platforms, the perspicuity score is not very high. The comments have been that the platform is considered very helpful once it has been configured and executed in the production environment, but the configuration phase seems to be harder than expected, because of the difficult of the modelling phase and the setup of the BRAIN-IoT Fabric. The low score for the perspicuity also driven the low attractiveness, which is affected by the perceived difficulty for configuration and setup of the whole platform. It is however important to notice the most part of the BRAIN-IoT Platform components have been developed from scratch or starting from low Technology Readiness Level (TRL) background assets. The consequence is that some more effort will need to be invested in order to improve the usability in terms of system setup. The good achievement is that the main novel characteristics of the platform have been well received and considered relevant and useful by the experts.

Figure 5 shows the positioning of the BRAIN-IoT Platform relative to the benchmark. The results show the good feeling w.r.t. the Novelty and Dependability, for which the score is Excellent. Considering the benchmark refers to solutions in every Information and Communication Technologies (ICT) field, meant to be commercial products, the curve of the BRAIN-IoT platform is in line with the expectation of a research and innovation action, where the maturity of the developed solution is still about around TRL 6, but the innovative aspects are well evident.

A similar evaluation has been performed to evaluate the software within the scope of the two application scenarios. When applied to the Service Robotics scenario, despite the perspicuity remains in line with the values determined before, the attractiveness is much higher. This is because the perception may change a lot when you think about the technology applied to a specific context, and the benefits that the platform could bring are much more evident. Basically, the stakeholder but himself in the shoes of the person who will benefit from the execution of the platform, instead of the IT manager who is supposed to install and setup the system. This means that, despite the BRAIN-IoT Platform continues to be evaluated as complicate to setup, it is considered good for managing swarm robotics applications.

Figure 6 shows the positioning of the BRAIN-IoT Platform relative to the benchmark. It shows even clearly how the BRAIN-IoT Platform is considered above the average in a context of SRWL. Instead, the dependability is decreased because of the security perspective in this context is more in line with the state of the art technologies. As for the SRWL scenario, a similar analysis could be made for the CIWDM. However, differently from the other scenario, here the perspicuity is higher: while for the SRWL scenario, the robotic applications developer cannot ignore the system setup phase, in the case of the management of the CIWDM, the platform is evaluated from the perspective of the pure end-user. Figure 7 shows the positioning of the BRAIN-IoT Platform relative to the benchmark. In this case, the platform has been evaluated as beneficial for managing a critical infrastructure, especially considering the security features and the resiliency capabilities.

8 CONCLUSION

BRAIN-IoT platform aims to pave the way of the research around the strict requirements of the next-generation IoT paradigm(AIOTI, 2020). In other words BRAIN-IoT platform is a first implementation of a meta operating system for the IoT domain, which facilitates the implementation of secure and self-adaptive IoT applications. The platform has been tested and applied to robotics scenarios in which BRAIN-IoT enables the self-controlled robots interact with the environment and adopt their behaviors correspondingly. In addition, BRAIN-IoT platform demonstrated its advanced features in industry and agile critical infrastructures management especially for the physical infrastructure monitoring, and abnormal behavior detection and prediction. Such meta operating system maps toward the 3D architecture defined by AIOTI but some functionalities still need to be either covered or enhanced, such as safety, trustworthiness. As part of the future works, the authors plan to extend the BRAIN-IoT platform implementing these functionalities with the aim to implement a full featured meta operating system for the IoT.

ACKNOWLEDGMENT

The research leading to these results has been supported by the European Union through the BRAIN-IoT project H2020-EU.2.1.1. Grant agreement ID: 780089.

REFERENCES

Adolphs, P. and Epple, U. (2015). Reference architecture model industrie 4.0 (rami4.0). Standard, ZVEI – German Electrical and Electronic Manufacturers' Association.

AIOTI (2020). High Level Architecture (HLA). Standard, AIOTI WG Standardisation. https://aioti.eu/wp-content/uploads/2020/12/ AIOTI_HLA_R5_201221_Published.pdf.

Basu, A., Bensalem, S., Bozga, M., Combaz, J., Jaber, M., Nguyen, T.-H., and Sifakis, J. (2011). Rigorous Component-Based System Design Using the BIP Framework. *IEEE Software*, 28(3):41–48.

Bauer, M., Boussard, M., Bui, N., Carrez, F., Jardak, C., Loof, D., Magerkurth, C., Meissner, S., Nettsträter, A., Olivereau, A., Thoma, M., Walewski, Stefa, J., and Salinas, A. (2013). Internet of things – architecture iot-a deliverable d1.5 – final architectural reference model for the iot v3.0. Technical report.

Chehida, S., Baouya, A., Alonso, D. F., Brun, P.-E., Massot, G., Bozga, M., and Bensalem, S. (2021). Assetdriven approach for security risk assessment in iot systems. In Garcia-Alfaro, J., Leneutre, J., Cuppens, N., and Yaich, R., editors, *Risks and Security of Internet and Systems*, pages 149–163, Cham. Springer International Publishing.

Chehida, S., Baouya, A., Bozga, M., and Bensalem, S. (2020). Exploration of impactful countermeasures on iot attacks. In *2020 9th Mediterranean Conference on Embedded Computing (MECO)*, pages 1–4.

Ghenassia, F. (2006). *Transaction-Level Modeling with Systemc: Tlm Concepts and Applications for Embedded Systems*. Springer-Verlag, Berlin, Heidelberg.

Gürgen, L., Munilla, C., Druilhe, R., Gandrille, E., and Nascimento, J. (2016). *sensiNact IoT Platform as a Service*, pages 127–147.

IEEE (2020). Ieee standard for an architectural framework for the internet of things (iot). *IEEE Std 2413-2019*, pages 1–269.

Lin, S.-W., Miller, B., Durand, J., Bleakley, G., Chigani, A., Martin, R., Murphy, B., and Crawford, M. (2019). The industrial internet of things volume g1: Reference architecture. Standard, Industry IoT Consortium. https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf.

Maillet-Contoz, L., Michel, E., Nava, M. D., Brun, P.-E., Leprêtre, K., and Massot, G. (2020). End-to-end security validation of iot systems based on digital twins of end-devices. In *2020 Global Internet of Things Summit (GIoTS)*, pages 1–6.

Rashid, M. R. A., Conzon, D., Tao, X., and Ferrera, E. (2019). Privacy Awareness for IoT Platforms: BRAIN-IoT Approach. In Ramos, J. L. H. and Skarmeta, A. F., editors, *Security and Privacy in the Internet of Things: Challenges and Solutions*, volume 27 of *Ambient Intelligence and Smart Environments*, pages 24–43. IOS Press.

Römer, L., Jeroschewski, S. E., and Kristan, J. (2020). Leveraging eclipse iot in the arrowhead framework. In *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, pages 1–6.

UML2 (2017). *Unified Modeling Language (Version 2.5.1)*. Object Management Group.

Vermesan, O. and Bacquet, J. (2018). *The Next Generation Internet of Things – Hyperconnectivity and Embedded Intelligence at the Edge*, pages 19–102. River Publisher.