OSDFramework: an Open-and-Secure data Framework to enable interoperable applications in IoT ecosystems

Rodrigo Elias Francisco[1,2], **Flávio de Oliveira Silva**[1]

[1]Faculty of Computer Science – Federal University of Uberlandia (UFU)
Uberlandia – MG – Brazil

[2]Goiano Federal Institute - Campus Morrinhos
Morrinhos - GO - Brazil

rodrigo.francisco@ifgoiano.edu.br, flavio@ufu.br

Abstract. *There is in the field of IoT the interest in innovating to allow the appearance of several applications with the great mass of data generated. However, there are difficulties regarding interoperability, security, and privacy involving data, platforms, and communication. Therefore, this article proposes OSDFramework, which implements the Open-and-Secure Data concept with a repository for semantically interoperable secure data sharing. The architecture for the framework is described and depends on the solution of challenges involving data transformations of different models for interoperability, semantic and privacy, and designing security protocols for sending and receiving data in the possible way concerned to the user.*

1. Introduction

The Internet of Things (IoT) is a theme worked by several academic and business institutions, as it enables innovations in different fields of application, such as E-Health and Industry 4.0. The interest in to use technology to control processes in the various domains has always existed, however, advances in electronics, computing, and data communication have made IoT viable, which will mass the use of technology.

Cloud Computing makes it possible to obtain economic and technical benefits, such as elasticity. There are scientific papers that address Cloud-IoT integration, for example, [Botta et al. 2016] mentioned research opportunities in this subject involving solving problems on Service Level Agreement, security, privacy and the need to improve the possibilities of migration between Cloud services.

Thus, a market was created around IoT technologies and applications that are organized in specific ecosystems involving certain business organizations that work with their already established standards and offer solutions with vertical integration regarding IoT and Cloud resources. This brings problems, e.g., situations where there is interest in creating IoT (System-of-Systems) applications that aggregate data from different Clouds that bring difficulties with semantic and technical interoperability since the standards have differences involving communication, security, privacy, format, and semantics of data related the Cloud. Thinking about the heterogeneity of IoT applications and communication infrastructures for IoT, the work of [Yaqoob et al. 2017] describes the interdependence of interoperability with scalability, flexibility, mobility, and security management.

This complexity in IoT research, involving many different factors such as data, hardware, software, communication, encourages the creation of experimentation environments. For example, the FIESTA-IoT project, according to [Nguyen et al. 2018], work towards a global IoT Experimentation-as-Service (EaaS) infrastructure/ecosystem, providing an experimental infrastructure with software, semantic techniques, processes of certification and best practices to facilitate the integration of IoT resources, testbeds infrastructure, and applications.

There is the use of specific patterns linked to open-data in the research, e.g., the [Dave et al. 2018] article worked around the integration between Building Information Modeling (BIM) and IoT, using the standardized Open Messaging Interface) and Open Data Format (O-DF). In spite of these technical difficulties, the use of open-data can be useful for the creation of these applications that consume data of different Clouds, being each Cloud related to a silo of data. However, it is necessary that the idea of open-data consider security. Therefore, this research introduces the concept of Open-and-Secure data applied to the IoT context.

The topic discussed in this paper addresses several application domains, however a use case is described for explanation, that it is an Intelligent City where there are several silos of data (such as transport, health, environmental monitoring) and there is the interest in creating an innovation ecosystem where new applications can arise from the consumption of such data.

This work is organized as follows: Section 2 describes related work regarding open-data. Section 3 describes the proposed framework and its mains requirements. Section 4 presents some final considerations and presents the future directions of this research.

2. Related Work

The literature presents important contributions and reflections for the development of this subject, since the use of open-data has already been perceived as being of interest to several IoT applications for some time. For example, the work of [Doukas and Antonelli 2014] explores a case of use of Smart Cities in the city of Barcelona on an application involving urban traffic and parking that used open data, still in this application domain the article of [Yacchirema et al. 2018] worked on a system intelligent for sleep monitoring that involved data on environmental pollution and climatic conditions related to the open data catalog of the city of Valencia in Spain, and on the other hand the work of [Kim-Hung et al. 2017] mentions the use of open data sources in Industrial Internet of Thing (IIoT).

Despite the possibilities that open-data brings about creating new applications composing data from others, there are security and privacy issues that are the targets of research projects. The FIESTA-IoT project presented by [Nguyen et al. 2018], eg, aims at an infrastructure/ecosystem for global IoT EaaS in order to allow experiments on multiple testbeds interoperably in a Cloud-IoT environment and applications that facilitate sharing (open-data) and reuse, it presents security aspects such as defining security by design and the use of an access control based on the session token on the service activation layer that allows the end user to directly interact with the structure by of web services.

The research of [Attila et al. 2016], to address the interconnection between IoT

and Health Information Systems with a Telemedicine Hub that supports open data, used an authentication and authorization mechanism, worked with randomly generated token for each Web request to validate and authorize the user and the Oauth authentication and authorization standard, and the definition and modification of data privacy parameters such as private, public, and anonymous. In addition, the Open Data protocol (OData) was used as a standard for creating and consuming queryable and interoperable terminals implemented with Representational State Transfer (RESTful) Application Programming Interface (API).

These concerns and definitions become more complex depending on the volume of data the system is working on, the type of information it is intended to generate, and the costs of computing and data communication, which in certain situations involves the use of Big Data and data analysis with advanced techniques of Artificial Intelligence and Data Mining. The work of [Mossucca et al. 2016], eg, proposed for the public transport domain, works with Big Data and the Extract Transform Load (ETL) concept, in order to obtain data from different sources as IoT devices and social network, transformation involving data cleansing and anonymization, and open data sharing, which indicates that security and privacy must properly be part of the architecture of any solution. However, these requirements are not always taken into account from the outset.

3. Proposed Architecture

The proposed strategy about open-data in order to share data from different IoT applications (with semantically different data silos) in a secure way involves the creation of a common cloud-deployable repository that receives, manages, and shares such data. Figure 1 illustrates the proposal with a situation that aims to create App#3 that uses data shared by IoT applications App#1 and App#2, which meets to the Smart City use case described in Section 1.

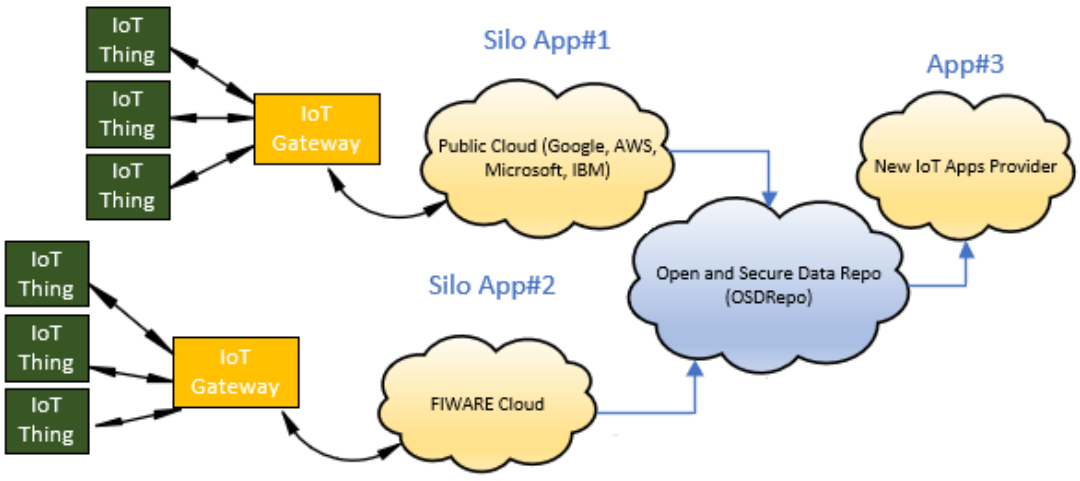

Figure 1. Creating App#3 with shared open data using the repository (OSDRepo)

To define the architecture, the following requirements have been proposed.

- Secure service to receive data

- Handle data with Common Data Model

- Translate Native Data Model to Common Data Model respecting privacy
- Allow maintain historical data (publish/subscribe mechanism)
- Write data in a secure way
- Read data in a secure way
- Access control and permissions to different cloud providers
- Secure service to share data
- Make integration process easy for both parties

The survey of these requirements made it possible to propose OSDFramework, which aims to enable IoT applications to open their data in a secure and controlled manner in order to contribute to the creation of new applications built using such data. The framework was thought for implementation in Cloud environments considering that such environments concentrate and store the IoT application data, which can be understood by the Figure 2 that describes the architecture of OSDFramework at a high level, in a way that not be difficult for both parties.

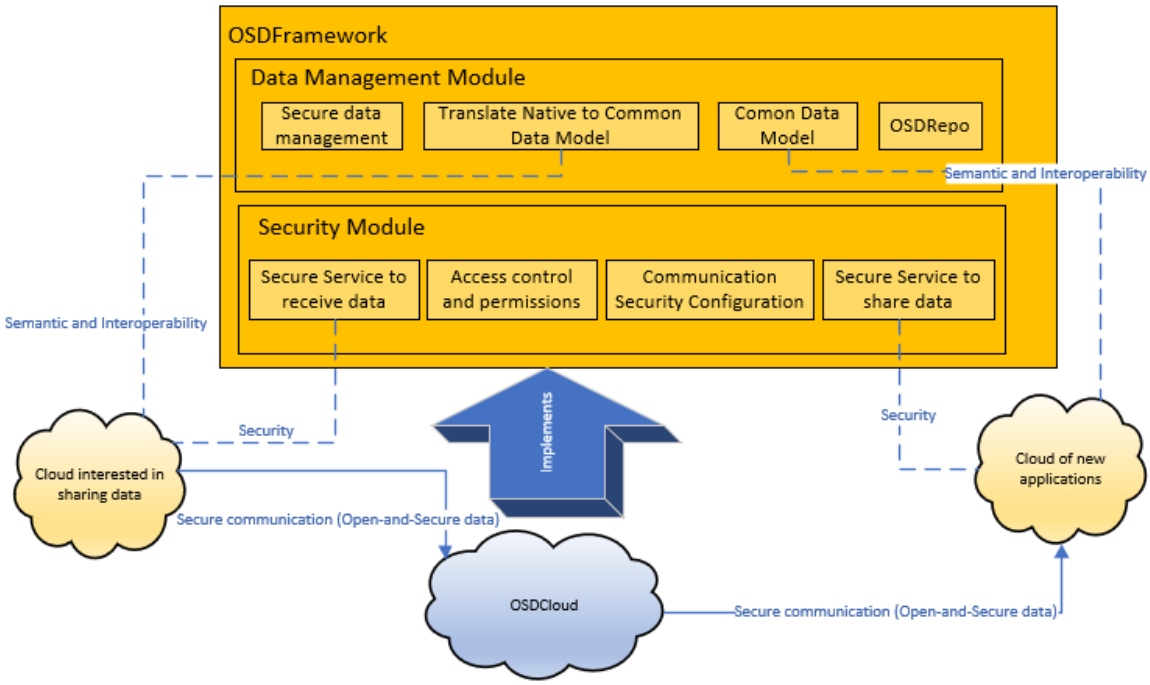

Figure 2. Architecture Design of OSDFramework

OSDFramework is divided into two modules, data management module and security module. The OSDFramework architecture was designed to deal with security and privacy issues in the process of sharing data related to the original IoT applications, since privacy eg can be achieved with strategies, e.g., the definition the appropriate granularity level of the data and the anonymization and security must be present in communication and data management. In order to be able to share data, OSDRepo has been proposed, which is a repository to open the data that is protected given the specification of the framework.

The security module includes the services of receiving and sending data and has been designed in such a way as to reduce the work of the parties with such interests. Stakeholders (to open data and receive open data) will use these services and will have to have in their computing environments resources to provide communication security (e.g. native cryptographic features) agreed with OSDCloud. In addition, the security module includes access control and permissions and the security configuration for communication agreed upon between the parties. The idea is, with these features, to flexibly work with security services, such as confidentiality, integrity, authenticity and protocols involved.

The data management module was conceived with the idea that data can come from different sources and each source have its own format and semantics, and therefore a common data model was defined that semantically represents the data to be made available in the repository and one translator from the native data model to the common data model that should consider data privacy issues. There is secure data management, which includes allowing to maintain historical data according to the publish / subscribe mechanism, and data writing and reading, which brings up research challenges on how to ensure security in this process.

4. Final Considerations and Future Directions

The idea that security should be part of the architecture discussion from the outset was used in designing this project. Thus, OSDFramework was thought of as a viable proposition, which implies being easy for entities that want to share and receive data, and secure. Several fields of application that want to innovate their ecosystem can benefit from the proposal, such as Smart Cities, Industry 4.0 and Health.

The next step of this project, which is already specified and with a defined architecture, is to solve the research problems and proceed with the implementation. The next few paragraphs present the problems to be solved.

Despite the high-level specification, it is necessary to deepen the security research applied to the framework. Security services, access control and permissions, security in sending and receiving data, protocols, encryption contribute to this step of the research. It is interesting to contribute to answer: How to define the most appropriate security configuration for a given use case?

The data management module also has challenges to be solved, such as the strategy to translate from the native data model to the common data model thinking about the diversity of schemas and technological details that may exist and computational cost thinking about an actual application.

The strategy to build the cloud repository is another important challenge. It is necessary to search in the literature the existing options that most attend the operations required for this project, such as reading and writing and with security guarantees.

References

Attila, A., Garai, Á., and Péntek, I. (2016). Common open telemedicine hub and infrastructure with interface recommendation. In *Applied Computational Intelligence and Informatics (SACI), 2016 IEEE 11th International Symposium on*, pages 385–390. IEEE.

Botta, A., De Donato, W., Persico, V., and Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future Generation Computer Systems*, 56:684–700.

Dave, B., Buda, A., Nurminen, A., and Främling, K. (2018). A framework for integrating bim and iot through open standards. *Automation in Construction*, 95:35–45.

Doukas, C. and Antonelli, F. (2014). A full end-to-end platform as a service for smart city applications. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2014 IEEE 10th International Conference on*, pages 181–186. IEEE.

Kim-Hung, L., Datta, S. K., Bonnet, C., Hamon, F., and Boudonne, A. (2017). An industrial iot framework to simplify connection process using system-generated connector. In *Research and Technologies for Society and Industry (RTSI), 2017 IEEE 3rd International Forum on*, pages 1–6. IEEE.

Mossucca, L., Goga, K., Spoto, G., Bolognesi, T., and Caragnano, G. (2016). Bussola: A cloud collaborative platform of oriented services to passengers. In *Complex, Intelligent, and Software Intensive Systems (CISIS), 2016 10th International Conference on*, pages 420–425. IEEE.

Nguyen, H., Serrano, M., Gyrard, A., and Tragos, E. (2018). Fiestaiot project: Federated interoperable semantic iot/cloud testbeds and applications. In *Companion of the The Web Conference 2018 on The Web Conference 2018*, pages 425–426. International World Wide Web Conferences Steering Committee.

Yacchirema, D. C., Sarabia-Jácome, D., Palau, C. E., and Esteve, M. (2018). A smart system for sleep monitoring by integrating iot with big data analytics. *IEEE Access*, 6:35988–36001.

Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., and Guizani, M. (2017). Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. *IEEE Wireless Communications*, 24(3):10–16.