Securing FIWARE with TEE technology

Luigi COPPOLINO [a,b], Roberto NARDONE [a,b], Alfredo PETRUOLO [a,b] and
Luigi ROMANO [a,b,c,1]

[a] *University of Naples "Parthenope", Isola C4, Centro Direzionale, 80143 Naples, Italy*
[b] *Trust UP, Via Francesco Petrarca, 80, 80122 Naples, Italy*
[c] *ICAR-CNR, Via Pietro Castellino, 111, 80131 Naples, Italy*
ORCiD ID: Luigi Coppolino https://orcid.org/0000-0002-2079-8713, Roberto Nardone
https://orcid.org/0000-0003-4938-9216, Alfredo Petruolo
https://orcid.org/0009-0003-2970-5864, Luigi Romano
https://orcid.org/0000-0003-2571-8572

Abstract. An important objective being pursued by the European Commission is the establishment of a unified data market where stakeholders can safely and confidently share and exchange data in standardized formats. This trend is supported by numerous initiatives, promoting the creation of European Common data spaces, and it is already in full swing in several sectors, such as energy and health. Among the many initiatives for building common data spaces, FIWARE appears to be one of the most promising. FIWARE promotes the use of Digital Twin technology to build distributed infrastructures for facilitating real-time data sharing in collaborative environments. By fostering an open and collaborative approach to software development and providing several building blocks of IT architectures for a number of domains (specifically: Smart AgriFood, Smart Cities, Smart Energy, Smart Industry, and Smart Water), FIWARE facilitates the creation of Digital Twins of real-world Industry 4.0 setups in a shared data space, which is typically hosted in the cloud. This paper addresses the security issues in a typical functional FIWARE architecture and provides a detailed description of a reference solution which ensures data confidentiality and integrity throughout the data life cycle, i.e. from the generation to the consumption phase. The proposed solution strongly relies on Commercial Off The Shelf Trusted Execution Environment technologies (namely: Intel SGX and Arm TrustZone) to provide effective protection of data-in-use. Protection of data-at-rest and data-in-transit is achieved by means of advanced cryptographic techniques and secure communication protocols, respectively.

Keywords. European Common Data Space, Confidential Computing, Data Protection, Cloud Architecture, Trusted Execution Environment

1. Rationale and Contribution

The European data strategy aims to bring together relevant data infrastructures and governance frameworks in order to facilitate data pooling and sharing while maintaining the control and ownership of the data by the companies and individuals who generated it. The governance of the European data spaces is rooted in European principles and legislation. Namely, the General Data Protection Regulation (GDPR) [1] and the Network

[1] Corresponding Author: Luigi Romano, luigi.romano@uniparthenope.it

and Information Systems Directive (NIS2) [2] address the free flow of data within a secure environment. Furthermore, the European Union has initiated and funded various programs and associations to promote the adoption of new data-driven technologies and achieve data sovereignty, such as The Interoperability Framework for Digital Services and Data (IDSA) [3], GAIA-X [4] and FIWARE [5].

IDSA encompasses a broad spectrum of issues regarding the interoperability of digital services and data, including technical standards, data formats, and semantic data models. It offers recommendations for the adoption of common technical standards and protocols for data exchange, as well as standards to facilitate data sharing through data spaces that have consistent rules, certified data providers and recipients, and mutual trust among partners. GAIA-X aims to tackle the obstacles facing the data landscape within the European Union. The design of GAIA-X is founded on the principle of decentralization, with various individual platforms adhering to a shared standard. The ultimate aim is to establish a data infrastructure that embodies the European values of openness, transparency, and trust, by constructing an interconnected system that links together Cloud Services Providers in many critical scenarios. At last, FIWARE contributes to the creation of dataspace by providing a comprehensive set of Application Programming Interfaces, which simplify the process of developing advanced applications.

FIWARE enables the development of Digital Twin solutions by using standardized data models that align seamlessly with Europe's perspective on interoperability within the data space. The Digital Twin solution serves as a critical data source for the dataspace, as it is widely adopted by the industry, the information collected and analyzed by Digital Twins hold great significance and in certain cases, it could be shared to create new services or to improve business lines of different providers [6]. From a cybersecurity perspective, the adoption of the Common European data space, the widespread use of Digital Twins, and the strong focus on the cloud architecture represent a significant increase in the overall attack surface available to malicious users. FIWARE offers several ad hoc components that address cybersecurity concerns related to authentication and identification procedures, including PEP Proxy and others. These components have undergone FIWARE approval and are categorized as GEs, available directly from the GEs catalogue. However, FIWARE does not currently provide guidelines or GEs to ensure data integrity and confidentiality during the data processing phase.

Several works in the literature analyze cybersecurity issues in the FIWARE architecture. However, most of them concentrate exclusively on topics related to transmission protocols and communication methods. The authors in [7] have incorporated a semi-autonomous method for authentication and identity management using certificates for FIWARE IoT devices. However, the proposed solution does not address the integrity and confidentiality of data-in-use. Furthermore, the authors in [8] proposed a technology-agnostic architecture to enable access and usage control in industrial data ecosystems, demonstrating its application in different scenarios. The proposed architecture has been implemented through the use of FIWARE GEs. However, this work also addresses concerns regarding data access and usage control and it does not provide adequate protection against potential attacks from high-privilege users. Another approach to increase the overall security of FIWARE is proposed in [9], where the authors designed and implemented a FIWARE Blockchain adapter to prevent data tampering with distributed ledgers by notarizing all the transactions from and to the FIWARE Context Broker (i.e., the component in charge of storing all the contextual information). Leaving out the possible cost increase, the proposed approach still does not solve the problem of protecting data in use. A first tentative of employing trusted execution environments to enhance overall trust and protection of data in use is described in [10], where the authors offer a new component for key management that can be used to provide privacy, confidentiality, and integrity guarantee for data. The component is proposed as a FIWARE GE and has been implemented relying on Intel SGX architecture.

This work aims at defining the conceptual model of a comprehensive FIWARE-compliant architecture that is able to protect data from generation to final usage. The proposal abstracts the Trusted Execution Environments (TEEs) for the protection of data in use with respect to specific technologies and adopts advanced encryption techniques to cover all other phases of the data security lifecycle. The rest of the paper is organized as follows. Section 2 provides the needed background on the enabling technologies. Section 3 conducts the security analysis and specifies the threat model. Section 4 describes in detail the proposed architecture, also giving a perspective on secure data communication. Section 5 ends the paper by giving some closing remarks.

2. Enabling Technologies

2.1. Digital Twin

A Digital Twin is a virtual replica of a physical system that is created using sensors, data analytics, and machine learning algorithms to capture and analyze real-time data from the physical system. Digital Twins are essential in Industry 4.0 such as to be considered capable of completely transforming the way physical objects and systems will be monitored, analyzed, and optimized [11]. Digital Twins enable engineers to use the increasing amount of data generated in real-time by the IoT devices to obtain valuable insights into how the systems operate, enabling their simulation, analysis and optimization to increase efficiency, productivity, and cost savings.

The process of building a Digital Twin involves several steps, including data acquisition, modelling, simulation, and deployment [12]. The first step in building a Digital Twin is data acquisition. This involves collecting data from sensors and other sources that are installed on the physical system. The data can include various types of information, such as temperature, pressure, speed, and other relevant parameters. The data is typically collected in real-time and stored in a cloud-based system for processing and analysis. The second step is modelling, where the data collected from the physical system is used to create a virtual model of the system. The third step is the simulation, where the virtual model is used to simulate the behaviour and performance of the physical system. The final step is deployment, where the Digital Twin is integrated with the physical system. The Digital Twin is connected to the sensors and other devices that are installed on the physical system, allowing real-time data to be collected and analyzed. Digital Twin modelling is an essential component of the European concept of data space. By providing a virtual representation of the physical system, Digital Twins enable real-time monitoring and optimization of performance, integration of data from different sources, and simulation of different scenarios. As such, Digital Twin modelling is a critical technology for organizations looking to improve the management and sharing of data across different domains and sectors. One of the key benefits of Digital Twin modelling in the context of data space is the ability to integrate data from different sources and domains. Digital Twins can be connected to a range of sensors and devices, enabling data to be collected from different parts of the physical system.

2.2. FIWARE

The FIWARE platform is grounded in the principle of interoperability. It enables the creation of new, smart digital solutions across a diverse range of critical sectors through its suite of GEs [13]. The platform offers a comprehensive set of Application Programming Interfaces, which simplify the process of developing advanced applications. The mission of FIWARE is especially significant in light of the fourth industrial revolution and the rapidly growing market for big data. At the core of its enabling technologies is the *Context Broker*, which has the capability of gathering and managing information in real-time to facilitate situational awareness and build a Digital Twin solution for monitoring systems and assets. This is made possible through the standardization of data, which is achieved through the efforts of the FIWARE Foundation and its partners. FIWARE primarily focuses on the world of the Internet of Things (IoT). To aid in connecting and managing IoT devices, the platform offers a range of dedicated GEs. Among these, the IoT Agent plays a crucial role as the core component for managing such devices [14]. It acts as a bridge between the IoT devices and the FIWARE platform, facilitating the translation of incoming messages, and enabling the processing and management of information through the context broker. The IoT Agent is designed to accommodate various communication protocols, such as MQTT, UltraLight and others. FIWARE also enables the creation of personalized IoT Agents, facilitating the connection of a wide range of devices. Regarding security considerations, the FIWARE marketplace provides several GEs to meet the privacy requirements of applications. The Identity Manager GE implements widely adopted standards such as OAuth 2.0 and OpenID Connect to ensure secure authentication. Additionally, the Key Rock GE provides authentication and authorization access to data using the latest encryption standards such as SSL/TLS. The PEP Proxy GE also plays a critical role in ensuring that all requests to access resources are properly authorized. The combination of these GEs contributes to the overall security of the platform. In this paper, two GEs have been taken into consideration, the Context Broker and IoT Agents. The ultimate objective is to establish a secure data architecture that ensures the confidentiality of the data that describes the modelled digital twin.

2.3. Trusted Execution Environment

Hardware-assisted security is widely used in Confidential Computing to protect data-in-use [15]. Trusted computing emphasizes predictable behaviour, contributing to secure systems alongside other components. It is defined by the Trusted Computing Group (TCG) as consistent behaviour for a specific purpose. Hardware-assisted trusted computing ensures reliable and intended machine behaviour through unique encryption keys stored in inaccessible hardware. The Chain-of-Trust (CoT) concept validates components up to the Root-of-Trust (RoT). Trust anchors within hardware components enhance security in hardware-assisted trusted computing, providing better defence against powerful attackers compared to software-based solutions. Overall, trusted computing combines predictable behaviour, hardware support, and validation mechanisms to build secure systems.

The TEE is a segment of the main processor found in connected devices. Its purpose is to ensure that sensitive data is securely stored, processed, and protected in a separate and trustworthy environment. The TEE provides a defence against software attacks that arise from high-privileged users. The TEE is ingrained within the CPU, enhancing protection against physical attacks, such as bus sniffing or cold boot. Unlike the TPM, the TEE features an extensive range of TC features, including an isolated execution area for sensitive code with curtained memory, which protects against runtime attacks like CRA (Code Reuse Attack). In recent years, two primary technological implementations of TEE have been introduced, which will be discussed below.

Arm TrustZone. Arm TrustZone is a security technology developed by Arm that enables the partitioning of the hardware and software resources of a System-on-a-Chip into secure and normal worlds. The normal world is also known as the non-secure world. This separation is achieved through an extended system bus design that adds a non-secure bit to bus addresses. The TrustZone Protection Controller configures resources as either secure or non-secure, while the TrustZone Address Space Controller assigns memory regions to either the secure or non-secure side. A TrustZone-enabled processor can switch between five modes, including the monitor mode, which allows for context-switching between virtual processor cores. The monitor mode can be entered from the normal world through normal interrupts, external aborts, or by calling the dedicated SMC instruction. When switching between worlds, the context of the world switching from must be saved and the one of the switching must be restored.

Intel Software Guard eXtensions (SGX). Intel SGX is the TEE solution offered by Intel. It uses a “reverse sandbox” approach to safeguard sensitive processes’ address spaces at the CPU level, even from the operating system. It accomplishes this by using secure enclaves, which are memory regions that only permit access by enclave-specific code, while encrypting and hashing their contents to prevent unauthorized access by other software, including privileged programs. The boundaries between enclave and non-enclave sections are established by the processor and prohibit unauthorized access attempts by unapproved processes. SGX enhances data security in cloud environments, although this sensitive data is transported via the internet, which necessitates the use of Remote Attestation (RA), a mechanism that validates a software’s trustworthiness running in a specific enclave. The RA workflow involves a third-party remote entity verifying that an enclave possesses a valid measurement hash, is running in a secure environment, and has not been tampered with. SGX provides both intra-attestation and inter-attestation services, allowing RA procedures to be performed between two enclaves residing on the same or different hosts, respectively. The secure channel is built between the two enclaves via a Diffie-Hellman key exchange during the remote attestation service. Performance of applications secured with SGX suffers an overhead that can be limited if specific mitigation actions are taken [16].

3. Security Analysis

The architecture proposed by FIWARE well suits the one adopted by cloud environments. Therefore, ensuring the security of a typical FIWARE implementation is crucial in preventing unauthorized access to critical data and protecting confidentiality. The primary threat that requires attention involves the targeted exploitation of users, leaving them vulnerable to account or service hijacking, which can lead to data breaches and financial harm. A skilled attacker can use malware or social engineering tactics, such as phishing and pretexting, to gain unauthorized access to confidential information. In an industrial setting, this could have disruptive consequences as the intruder gains control of the broker and injects false data to deceive incident response teams. Additionally, internal users working as owners of a particular virtual machine (VM) instance can exploit the hypervisor to launch an attack on another VM instance hosted on the same server. Such a side-channel attack can compromise data integrity and confidentiality, potentially leading to data breaches. At last, malicious insiders can gain direct access to the underlying hardware and compromise sensitive user data, resulting in a heightened threat of data breaches. Additionally, the lack of visibility and control over data that is in use presents another challenge for data protection. While data at rest and in transit can be encrypted and controlled, data being actively used may be outside the scope of traditional security measures, putting sensitive information at risk of interception and exploitation by cybercriminals. To improve data security in use, solutions that protect data in real-time, without compromising usability or efficiency, are required. In FIWARE, the context broker is typically deployed in cloud environments, trusted computing techniques can be considered to establish a root of trust, ensuring data-in-use protection.

Threat Model. The threat model assumes the FIWARE deployed on a hosting infrastructure managed by a third party (e.g., cloud service provider); it means that both the Context Broker and IoT Agents run on a single node (from now on *FIWARE node*) under the control of an external actor. According to the literature, the *FIWARE node* host is a semi-honest adversary represented as an honest-but-curious model, which well describes a possible curious nature of a cloud service provider. As a result, the *FIWARE node* host has access to the Context Broker, leading to possible breaches of confidentiality and potential data exposure. Hence, when managing sensitive information, both applications and IoT devices need to trust the execution environment in which the *FIWARE node* executes. This requires authentication before sending data (for IoT devices) and retrieving data (for applications).

With respect to the IoT devices, we assume two different execution platforms model, trusted and untrusted. In the trusted platform model, the FIWARE context broker can rely on the authentication information provided by the device itself. However, even in such a model, there are three possible threats. Firstly, when data leaves an IoT device, it must be avoided for an attacker to intercept and access sensitive information, leading to the challenge of data-in-transit protection. Secondly, when data is stored at the context broker, it must be avoided that the attacker may use advanced techniques, like hypervisor attacks, to gain access to the FIWARE node host and retrieve the stored information. Lastly, when data leaves the context broker and reaches the application, measures must be taken to ensure the rights of the application to obtain the data.

In the untrusted platform model, the *FIWARE node* cannot trust the identity provided by an IoT device. Identity could be falsified and malicious data sent to the Context Broker, or the device itself could be tampered with or spoofed to inject false data into the context broker. This emphasizes the importance of securing data provided by authenticated devices. Additionally, also in the untrusted platform model, the same issues described above related to protecting data in transit and at rest must be addressed.

At last, the applications that need to obtain and process data are assumed to execute on untrusted platforms, arising similar issues for the identity management and the protection of data in use, as described for the IoT device exist.

Requirement Elicitation. Our proposal aims at building a novel architecture based on FIWARE with the goal of safeguarding data from the generation to the usage phase. Hence, each component of the architecture needs authentication and confidential computation guarantees before sensitive data are shared.

According to the threat model, the proposed architecture must avoid the *FIWARE node* host can access the user's data, also when it is processed. The potential to access, manipulate, or leak user data makes this a significant concern for organizations handling sensitive data such as financial information, healthcare records, and personally identifiable information. The proposed architecture should adopt TEE solutions to fulfil this requirement, enabling a process of users' data within a secure environment provided by TEEs. The host only should access encrypted data, and cannot access or manipulate it without the user's permission. Moreover, the *FIWARE node* host could be targeted by hackers, which puts the users' data at risk. However, with the usage of hardware-proof security, the *FIWARE host* node does not have any responsibilities in terms of the user's data. This means that even if hackers gain access to the node, they cannot access the user's data.

With respect to IoT devices, in both trusted and untrusted platform execution models, after the authentication phase, each device may encrypt data prior to transmitting it to the Context Broker or ask this functionality to the *FIWARE node*. The transmission of sensitive data must employ secure protocols like HTTPS to prevent data exposure during transfer. The encryption of data should also guarantee high-level security when data is at rest at the Context Broker. At last, data should be decrypted and utilized without being exposed to potential attackers or the *FIWARE node* host. TEE solutions could offer a viable way to solve this last issue.

4. Secured FIWARE Architecture

The proposed architecture must cope with the concerns about security in terms of confidentiality and integrity of the data previously discussed. Currently, the FIWARE ecosystem lacks a GE to manage confidentiality in the cloud environment, which leaves the data vulnerable to potential breaches. There are also unaddressed issues related to insider attacks by privileged users, such as super users, who have unrestricted access to the cloud environment. Moreover, authentication issues and identity management should be improved with respect to the current status of existing FIWARE GEs. In fact, there are specific GEs enabling the users' identity management which cope with the final users' authentication. The current FIWARE ecosystem lacks solutions specifically tailored for IoT systems addressing the identification and mutual authentication among components involved in the architecture.

4.1. Main components

Before describing the secured solution, it is needed to clarify the functional architecture considered in this work. Figure 1 depicts and details the components involved within the architecture, which are:

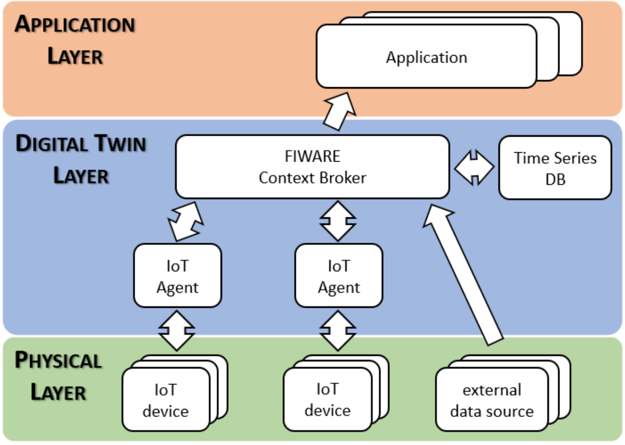

Figure 1. Functional Architecture.

- IoT device: a device collecting data.
- IoT Agent: a FIWARE component creating a universal interface to the Context Broker and performing the needed adaptation and normalization actions.
- Context Broker: the FIWARE Context Broker is used to store data coming from the IoT devices, providing a (data-based) Digital Twin of the physical system.
- Time Series DB: the database in which data coming from the IoT device is stored.
- Application: a generic application consuming data coming from the Context Broker.

As depicted by the figure, where the data flows are represented by the arrows, components are organized in a typical three-tier architecture. Starting from the bottom of the figure, the *Physical Layer* includes the IoT devices that are spread through the system; the *Digital Twin Layer* includes all the components needed to manage the Digital Twin of the system; the *Application Layer* includes the applications that aim at using data to provide value to the final users.

To address the security concerns raised by the lack of data protection mechanisms in the FIWARE ecosystem, Trusted Execution Environments (TEEs) have been employed to secure the proposed architecture. TEEs provide a secure and isolated environment that is resistant to attacks by even privileged users, thereby enabling the secure processing of sensitive data in the environment described in the trust model [17].

Different TEEs are needed in the architecture, as depicted in Figure 2. Starting from the bottom of depicted architecture, TEEs are needed in the IoT devices executing on untrusted execution platforms. In fact, unlike the other case considered for the device in the threat model, in this situation, the *FIWARE node* cannot trust the provided identity and the data, so it needs to attest and trust only information coming from an on-board TEE. Moreover, the same TEE can be also useful to run on-board encryption. Similarly, IoT Agents dealing with sensitive information need to be equipped with a TEE. In fact, even when IoT devices encrypt the data previously sending it to the *FIWARE node*, these components interact with the Key Manager to obtain the cryptographic keys. Also, they can be asked to encrypt sensitive data when devices are not able to perform this functionality. Of course, the Key Manager, which is the main component of the secured architecture

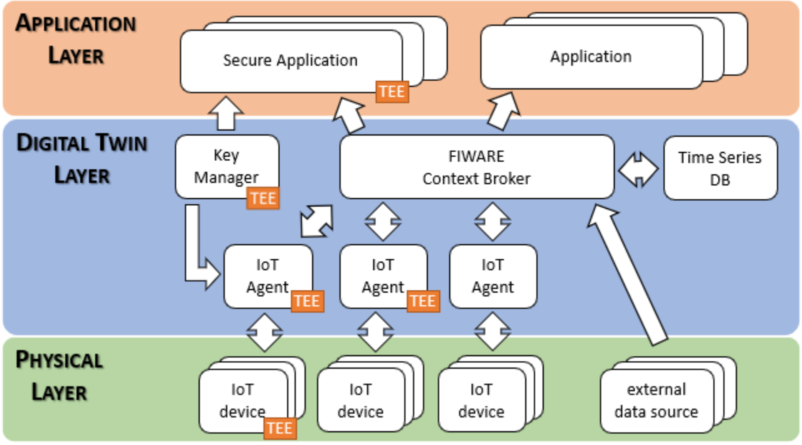

Figure 2. Secured Architecture.

in charge of providing encryption and decryption keys to the responsible components, must run entirely within a TEE. At last, secure applications (i.e., applications that need to access sensitive information) need to securely decrypt the information and process it within a TEE. Note that the FIWARE Context Broker and the Time Series DB do not need to execute partly or entirely in a TEE since they manage only encrypted data.

4.2. Secure Data Flow

When dealing with sensitive information, IoT devices need to be previously authenticated. IoT devices equipped with TEE can store their identity within the TEE and they can be authenticated via remote attestation. This approach facilitates the direct assignment of a secret key for encryption/decryption by the key manager. It is important to note that all data transmissions occur through the HTTPS protocol to prevent potential man-in-the-middle attacks. Once the data reaches the IoT Agents (equipped with TEE), the encryption process begins and the message payload is secured. The IoT agent, then, converts the message structure into a FIWARE-compliant NGSI (v2 or LD) format. This process enables the Context Broker to handle and store the transmitted data in the database.

To perform analysis on sensitive encrypted data, a generic application uses the subscription method to access the Context Broker data. This method entails the Context Broker notifying the subscriber of any data modifications and subsequently sending the data to them. The secure application must be equipped with a TEE solution, such as Intel SGX, within which data will be decrypted using the secret key provided by the key manager. The application is also authenticated by a remote attestation process and requires the key of decryption directly from the key manager. The processing of data will also take place in the TEE, guaranteeing that the data is always kept secure even during usage and processing. Figure 3 shows the sequence diagram of the secure dataflow from the generation to the FIWARE context broker and Figure 4 from the Context Broker to the secure application. The red rectangles within the figure include interactions within TEEs.

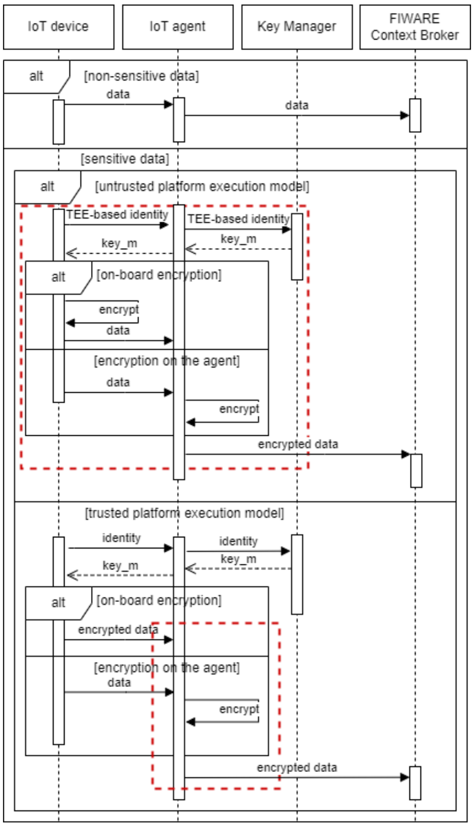

Figure 3. Secure data flow from the IoT device to the Context Broke

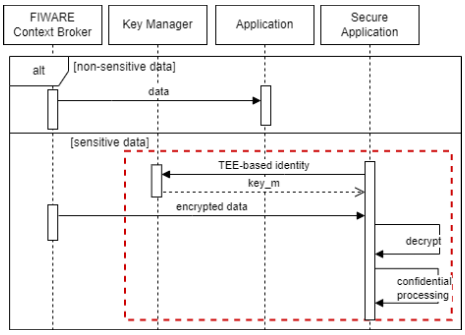

Figure 4. Secure data flow from the Context Broker to the Application.

4.3. Preliminary Evaluation

To support our proposal, we conducted a preliminary performance analysis deploying the context broker on a cloud-based Azure DCsv3 series virtual machine. The virtual machine utilizes 3rd Generation Intel Xeon scalable processors with Intel Turbo Boost Max Technology 3.0 and 32 GB of RAM. These processors have a base core frequency of 2.8GHz and are capable of reaching speeds up to 3.5GHz with Turbo Boost. We performed tests by deploying the context broker within and outside an SGX enclave, measuring the average latency with a fixed number of requests (10 requests per second) and a varying number of clients making GET requests to the context broker. By comparing the latency results between the enclave and non-enclave deployments, we aimed to assess the potential benefits and performance differences. Furthermore, despite the observed increase in average latency when deploying the context broker inside the SGX enclave, it is important to consider the trade-off in terms of the enhanced security provided. While the latency may be slightly higher, the significant gain in security measures offered by the enclave outweighs this impact. In figure 5 the results are shown. During our preliminary performance evaluation, we observed an average latency loss of 9%. It is important to note that this evaluation serves as an initial assessment and our intention is to conduct a more comprehensive performance evaluation of the proposed architecture in future works.

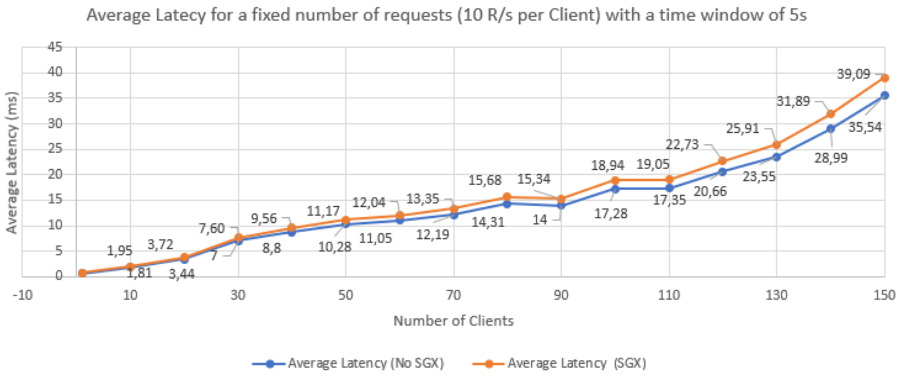

Figure 5. Average Latency of Orion Context Broker with Varying Numbers of Clients Making Fixed 10 Requests per Second.

5. Conclusions and Future Work

This paper provides a comprehensive overview of a secure implementation of FIWARE. The European Commission's new trend of establishing a Common European data space presents an opportunity to create a collaborative environment where sharing and exchanging data can benefit all stakeholders and improve business by providing new services. The focus is on the digital twin solution, which is a crucial technology that fuels the European Common dataspace. Specifically, FIWARE is discussed as an enabling technology for building the dataspace by providing APIs for developing Digital Twins solutions. This paper aims to emphasize the insufficiency of cybersecurity measures in the FIWARE architecture, which relies strongly on the cloud, in countering attacks during data usage and to propose a potential solution that ensures the protection of data right from its creation until its eventual use. To reach this objective Trusted Execution Environment solutions are discussed, and the importance of trust and security issues in cloud environments are analyzed.

Future work includes a security analysis and a deep testing campaign aimed at evaluating the performance of the proposed architecture in different realistic use cases. The evaluation can include various environments such as different contexts to test the architecture's robustness against various security threats. Furthermore, the scalability of the architecture and performance will be evaluated. Moreover, the deployment of the innovative components of our architecture as FIWARE GEs is included in future work.

Acknowledgements

This research has partially received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement No. 101070670 (EN-

CRYPT - A Scalable and Practical Privacy-preserving Framework) and partially from the Horizon 2020 Research and Innovation Programme under Grant Agreement No. 101020560 CyberSEAS. The content of this publication reflects the opinion of its authors and does not, in any way, represent the opinions of the European Union. The European Commission is not responsible for any use that may be made of the information that this publication contains.

References

[1] C. Tankard, "What the gdpr means for businesses," *Network Security*, vol. 2016, no. 6, pp. 5–8, 2016.

[2] A.-V. Dragomir, "What's new in the nis 2 directive proposal compared to the old nis directive." *SEA: Practical Application of Science*, vol. 9, no. 27, 2021.

[3] A. Braud, G. Fromentoux, B. Radier, and O. Le Grand, "The road to european digital sovereignty with gaia-x and idsa," *IEEE network*, vol. 35, no. 2, pp. 4–5, 2021.

[4] S. Autolitano and A. Pawlowska, "Europe's quest for digital sovereignty: Gaia-x as a case study," *IAI papers*, vol. 21, no. 14, pp. 1–22, 2021.

[5] V. Araujo, K. Mitra, S. Saguna, and C. Åhlund, "Performance evaluation of fiware: A cloud-based iot platform for smart cities," *Journal of Parallel and Distributed Computing*, vol. 132, pp. 250–261, 2019.

[6] A. Fuller, Z. Fan, C. Day, and C. Barlow, "Digital twin: Enabling technologies, challenges and open research," *IEEE access*, vol. 8, pp. 108 952–108 971, 2020.

[7] P. R. Sousa, L. Magalhães, J. S. Resende, R. Martins, and L. Antunes, "Provisioning, authentication and secure communications for iot devices on fiware," *Sensors*, vol. 21, no. 17, p. 5898, 2021.

[8] A. Munoz-Arcentales, S. López-Pernas, A. Pozo, Á. Alonso, J. Salvachúa, and G. Huecas, "Data usage and access control in industrial data spaces: Implementation using fiware," *Sustainability*, vol. 12, no. 9, p. 3885, 2020.

[9] S. Loss, H. P. Singh, N. Cacho, and F. Lopes, "Using fiware and blockchain in smart cities solutions," *Cluster Computing*, pp. 1–14, 2022.

[10] D. C. G. Valadares, M. S. L. da Silva, A. E. M. Brito, and E. M. Salvador, "Achieving data dissemination with security using fiware and intel software guard extensions (sgx)," in *2018 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 2018, pp. 1–7.

[11] D. M. Botín-Sanabria, A.-S. Mihaita, R. E. Peimbert-García, M. A. Ramírez-Moreno, R. A. Ramírez-Mendoza, and J. d. J. Lozoya-Santos, "Digital twin technology challenges and applications: A comprehensive review," *Remote Sensing*, vol. 14, no. 6, p. 1335, 2022.

[12] G. N. Schroeder, C. Steinmetz, R. N. Rodrigues, R. V. B. Henriques, A. Rettberg, and C. E. Pereira, "A methodology for digital twin modeling and deployment for industry 4.0," *Proceedings of the IEEE*, vol. 109, no. 4, pp. 556–567, 2021.

[13] F. Cirillo, G. Solmaz, E. L. Berz, M. Bauer, B. Cheng, and E. Kovacs, "A standard-based open source iot platform: Fiware," *IEEE Internet of Things Magazine*, vol. 2, no. 3, pp. 12–18, 2019.

[14] I. Zyrianoff, A. Heideker, L. Sciullo, C. Kamienski, and M. Di Felice, "Interoperability in open iot platforms: Wot-fiware comparison and integration," in *2021 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2021, pp. 169–174.

[15] L. Coppolino, S. D'Antonio, G. Mazzeo, and L. Romano, "A comprehensive survey of hardware-assisted security: From the edge to the cloud," *Internet of Things*, vol. 6, p. 100055, 2019.

[16] G. Mazzeo, S. Arnautov, C. Fetzer, and L. Romano, "Sgxtuner: Performance enhancement of intel sgx applications via stochastic optimization," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 4, pp. 2595–2608, 2022.

[17] L. Coppolino, S. D'Antonio, G. Mazzeo, L. Romano, I. Bonetti, and E. Spagnuolo, "The protection of lp-wan endpoints via tee: a chemical storage case study," in *2021 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, 2021, pp. 345–352.