ONE4ALL - Agile and modular cyber-physical technologies supported by data-driven digital tools to reinforce manufacturing resilience

Project nr: **101091877**

D3.2 Guidelines for a secure and open-source AI-based IOP

Version: 1.0

Funded by the European Union

ONE4ALL project is funded by the European Union under the Grant Agreement No 101091877. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Characteristics of deliverable	
Title	ONE4ALL
Partner	SDU
Contributors	IDE, AUTO, INO, KIT
Short description of deliverable	Guidelines for a Secure and Open-source AI-Based Intelligent Orchestration Platform and Its Technologies.
Submission date	31/10/2023
Type	Report
Audience	Public
Key words	Security guidelines; Secure architecture; Protection mechanisms; Intelligent orchestration platform

ONE4ALL Key Facts

Acronym	ONE4ALL
Project title	Agile and modular cyber-physical technologies supported by data-driven digital tools to reinforce manufacturing resilience
GA n°	101091877
Starting date	01/01/2023
Duration-months	48
Call (part) identifier	CLIMATE NEUTRAL, CIRCULAR AND DIGITISED PRODUCTION 2022 (HORIZON-CL4-2022-TWIN-TRANSITION-01)
Type of Action	HORIZON-RIA HORIZON Research and Innovation Actions
Topic identifier	HORIZON-CL4-2021-TWIN-TRANSITION-01-03
Consortium	11 organizations, all EU Member States
Model GA type	HORIZON Action Grant Budget-Based

ONE4ALL Consortium Partners

N.	Partner	Acronym	Country
1	IDENER RESEARCH & DEVELOPMENT (Coordinator)	IDE	ES
2	INNOPHARMA TECHNOLOGY	INO	IE
3	CRIT	CRIT	IT
4	EXELISIS	EXE	GR
5	UNIVERSITY OF SOUTHERN DENMARK	SDU	DEN
6	AUTOMATIONWARE	AUTO	IT
7	MADAMAOLIVA	MOL	IT
8	HOLOSS	HOLO	PT
9	DORTMUND UNIVERSITY	TUDO	DE
10	ORIFARM	ORI	CZ
11	KARLSRUHE INSTITUTE OF TECHNOLOGY	KIT	DE

Executive Summary

This document is aimed to provide all necessities to ensure a secure and open-source infrastructure for the IOP. It specifically focuses on offering guidelines on how to secure the IOP tools, data, digital modules and services, physical devices, and the network that interconnects all these components. The document first revises existing regulations and policies, both from industry and academia. This is done to ensure the best security measures suitable for the IOP infrastructure are adopted and implemented. Subsequently, a brief look into potential attacks that the IOP infrastructure might be susceptible to is performed. This review is followed by introducing adequate protection mechanisms to mitigate such attacks and secure the entire IOP infrastructure against cyber threats.

The document further provides guidelines to be followed and implemented accordingly. It delineates such guidelines into the different facets of the IOP. Thus, ensuring all components within the IOP ecosystem are captured in the guides. The document also emphasizes that proactive security measures are first put in place for the protection of the entire IOP prior to reactive measures. The security measures also adopt a comprehensive approach towards ensuring the protection of both IT and OT paradigms within the entire IOP. As a result, the guidelines effectively capture all essential security measures that would efficiently mitigate different attack scenarios. Finally, ethical considerations of user privacy in the use of open-source AI within the IOP are also addressed.

This version of the deliverable results from Task 3.2, which mainly handles the guidance towards a secure IOP. The second deliverable in M30 of the same task will ensure the implementation of the adopted guides and security measures. Therefore, it is worth nothing that the guides and protection mechanisms will be constantly reviewed and updated during the project execution phase as the task advances. This will make sure new and evolving threats are detected and mitigated with up-to-date security measures and techniques. Hence, guaranteeing the entire IOP ecosystem stays abreast and secure proof against all forms of cyber threats.

Table of contents

List of acronyms

IOP	Intelligent Orchestration Platform
AI	Artificial Intelligence
RCPM	Reconfigurable Cyber Physical Production Module
IT	Information Technology
OP	Operational Technology
IoT	Internet of Things
IIoT	Industrial Internet-of-Things
GDPR	General Data Protection Regulation
NIST	National Institutes of Standards and Technology
CISA	Cybersecurity and Infrastructure Security Agency
ISO/IEC	International Organisation for Standardization/Institute of Electrotechnical Commission
ETSI	European Telecommunication Standard Institute
ENISA	European Union Agency for Network and Information Security
EU-NISR	EU Network and Information Systems Regulations
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
SSL	Secure Shell
VPN	Virtual Private Network
RBAC	Role-Based Access Control
NAT	Network Address Translation
OSI	Open Systems Interconnection
DSN	Digital Supply-Chain Network
SMEs	Small and Medium-sized Enterprises
VLANs	Virtual Local Area Networks

List of figures

List of tables

1. Introduction to a Secure and Open-Source AI-Based IOP

This report provides guidelines for a secure and open-source infrastructure for the IOP. It highlights the security measures to be followed, protection mechanisms to be implemented, and AI-based ethics for the open-source IOP that will be observed during the execution phase of the project. The project interacts with several regulations and policies to deduce detailed procedures and protocols for a secure IOP. This is so that ONE4ALL can meet the required standard for secure infrastructure according to Industry 4.0. Further, D3.3 will revise the measures to ensure they are implemented and use them as the foundation for the project's security guidelines. These guidelines and protection mechanisms are tailored towards ensuring the security of the entire IOP tools and infrastructure based on an in-depth look into the architectural design of the IOP described in D3.1.

The deliverable D3.1 provided a comprehensive presentation of the technological scouting surrounding the IOP tools and architecture; D2.1 gave the general architecture of the digital twin and data requirements; D7.8 created the guide on how to process and manage data generated during the project execution; and D7.7 highlighted some gender and ethical concerns. WP3 deliverables, 1st D3.2 and D3.3 in M30, will be built on all these subsequent tasks in order to ensure all defined data, tools, infrastructures, etc. within the deliverables are secured and protected from cyber threats. The ethical concerns will also be addressed to ensure users' privacy from the use of AI.

1.1. *A Secure IOP Infrastructure*

The IOP infrastructure is considered the backbone of the ONE4ALL project, where data is received from digital devices within the manufacturing industry. It is then processed, stored, and/or transmitted to the relevant tools and applications for different purposes. The IOP also manages the streamlined interoperability between different systems and datatypes while facilitating the operation of data-driven digital twins, delivering valuable insights, and boosting end-users' decision-making. Hence, considering the important role the IOP plays in the ONE4ALL project, the significance of ensuring its protection is also critical.

Without the required protection in place, the IOP tools and its infrastructure can be vulnerable to several nefarious cyber-attacks, such as DDoS, malware injection, spear phishing, SQL injection, ransomware, kit exploits, etc. Thus, ruining the work built and data generated in several years within just a few minutes. Therefore, to ensure the security of the IOP infrastructure, its relevant tools and applications, as well as all data associated with it, different protection mechanisms will be adopted.

Moreover, to ensure the required protection is achieved, this deliverable will provide the security measures and guidelines that should be followed and implemented using a set of strong and robust protection mechanisms put together for the IOP tools and infrastructure. The security of the IOP will integrate the use of different technologies in order to achieve this. Such technologies will be adopted and implemented within the IOP network, data, tools, and infrastructure. The key protection mechanisms to be used include role-based access control, user authentication, monitoring and incidence response, network security, data security based on data access control, data usage audit, data leak prevention, data compliance, and data protection using an encryption technique.

The following are brief insights into what each chapter of this document offers.

Chapter 2 opens with a survey of existing guidelines and standards from both industry and academia. This will help us gain an insight into the general overview of other security measures and protocols and see what suits best for the IOP tools and infrastructure.

Chapter 3 begins with a brief look at the attacks the IOP can be susceptible to. It then delves into the protection mechanisms that would be used to mitigate cyber threats against the IOP tools and infrastructure while providing the required protection.

Chapter 4 provides the guidelines to be adopted and followed during the implementation of the protection mechanisms. This is done in consideration of each protection mechanism that would be used for the protection of the IOP tools and infrastructure.

Chapter 5 looks into the AI-based ethical considerations that must be adhered to in relation to the security and transparency/trustworthiness of systems and tools within the IOP and the entire ONE4ALL. And finally, Chapter 6 gives the general conclusion.

1.2. *Aim and Objectives*

The main aim of this deliverable is to provide guidelines and recommendations to ensure the security of the entire IOP data, tools, digital services and modules, network devices, interconnectivity, and cloud database, that will be observed and implemented throughout the project.

The key objectives of these guidelines are:

- Data protection and backup: Ensure that all sensitive data associated with the project is well managed, stored, and secured from unauthorized access, theft, and loss.
- Digital tools and module protection: Ensure that all digital tools, modules, and services associated with the IOP are well protected from unauthorized use by third parties and users that do not have the relevant access privileges.
- Systems protection: Ensure all operational systems and devices, such as cobots, sensors, cameras, and scanners associated with the IOP, are protected and secured.
- Network device protection: Ensure that all network devices, such as routers, firewalls, servers, etc., that aid with the network connection between different IOP tools and modules are secured.
- Interconnectivity protection: Ensures that the network connecting different tools and modules, as well as systems managed by the IOP, are secured from all forms of network breaches. Also, ensure the network connection provided by the IOP to the cobots sensors, scanners, cameras, and other devices is secured. In other words, the communication and transmission channels between the IOP and all other systems, tools, and devices are secured against cyber threats.
- Secure protocol: An outline of how all these protection mechanisms will be observed and implemented accordingly.
- AI-based ethical considerations: Ensure ethical considerations of AI with respect to the security, privacy, and trustworthiness of all systems.

2. Existing Guidelines and Best Practices

To compile a comprehensive list of best guides and practices, as well as have a general overview of other protocols and see what will suit best for the IOP, this section analyzed different existing recommended security measures, keeping in mind the constant evolution of IoT infrastructures to meet Industry 4.0 requirements. Hence, the guides provide us with insight to identify what must be protected within the IOP and to design suitable security protocols to prevent cyberattacks. This brings forth a literature review conducted in both academic and industrial settings, backed by the relevant government regulatory agencies.

Although there is currently no established comprehensive systematic framework for addressing security needs in the IIoT, the industry realized the need for standards in the early 2010s and subsequently proposed a number of recommendations. Since then, several guidelines and standards in the field of IIoT security and privacy provide manufacturers and users with guidance to improve security and privacy within the interconnected IIoT ecosystem. These guides have helped mitigate against several attacks that the IIoT are prone to, such as spoofing, spear phishing, malware, SQL injection, DDoS, etc. However, our exploration is mainly limited to the state-of-the-arts amongst these guides and standards, with consideration given to: The rapid development of the IoT industry that may have rendered some ideas ineffective, though current studies regularly refer to and align with those of the past in crucial security domains. In addition to evaluating reports and articles, standard and best practices developed by credible associations such as NIST, ISO/IEC, and EU-ETSI or manufacturing bodies such as ENISA and CISA were assessed. All these were backed by government agencies to ensure full security and privacy compliance laid by the relevant authorities.

2.1. *Survey of Guides and Regulations by Organizations*

2.1.1. National Institute of Standards and Technology (NIST)

The US Department of Commerce's National Institute of Standards and Technology (NIST) published its first report titled "IoT Device Cybersecurity Capability Core Baseline" (NIST IR 8259A) in 2020 [1]. The authors define a core baseline for the cybersecurity capabilities of an IoT device as a collection of device capabilities that are often required to facilitate overall cybersecurity measures aimed at protecting infrastructure, systems, and data. The recommended benchmark is the outcome of a collaborative endeavor aimed at developing a comprehensive inventory that reflects shared capabilities [1]. The document also outlines measures designed to boost the security of manufacturing industry and its products, thereby decreasing the number of IoT devices that have been compromised. Nevertheless, the guide fails to provide implementation procedures for these guidelines. However, the recently updated version of these guidelines (NIST IR CSF-2.0) [2] is focused on improving the implementation of cybersecurity in critical infrastructures. The framework proposed in the guide has been widely used to reduce cybersecurity threats in different manufacturing use cases.

2.1.2. European Union Agency for Network and Information Security (ENISA)

European Union Agency for Network and Information Security (ENISA) is another organization that has released numerous reports on the advancement of IoT security in industry. In 2017, the document "Baseline Security Recommendations for IoT" was published [3]. This project's objective was to acquire a deeper understanding of the security requirements of the IoT, with a particular emphasis on critical information services and infrastructure. The study offers an in-depth assessment of contemporary cybersecurity threats and an extensive set of protective measures for IoT devices. The authors compiled a list of recommendations, best practices, expert opinions, and industrial cyber security measures according to their findings. They further provide another guide specifically for

securing the IoT [4]. The work encompasses a comprehensive compilation of additional IIoT security standards, which could count as an invaluable initial resource for further investigations. It also incorporates standards from a variety of sources, including the ISO/IEC.

2.1.3. European Telecommunications Standards Institute (ETSI)

The European Telecommunications Standards Institute's (ETSI EN-303 645) guideline on cyber security for the consumer IoT is another important resource for securing IoT devices [5]. The document centers primarily on European regulations and seeks to establish an initial framework for IoT device production. It references several important projects, consisting of NIST and ENISA. In one of the initiatives, for example, it is striving to develop a framework to handle encrypted credentials in a complex setting of multifaceted devices. Consequently, manufacturers, executives, and experts rather than individual consumers are the intended audience. Recently, they also proposed an implementation guide for the consumer IO devices ETSI TR 103 621 [6]. The document provides guidelines to assist manufacturers and other relevant stakeholders in fulfilling the cyber security requirements established for Consumer Internet of Things (IoT) devices (ETSI EN-303) 645.

2.1.4. International Organization for Standardization/Institute of Electrotechnical Commission (ISO/IEC)

The recently published International Organisation for Standardization/Institute of Electrotechnical Commission (ISO/IEC 27400:2022) document provides guidelines on risks, principles, and controls for the security and privacy of IoT solutions [7]. The document gives an in-depth analysis of risk sources for IoT systems while suggesting a plethora of security and privacy solutions to help mitigate any form of cyber threat. The document also provides best practice recommendations to facilitate compliance with GDPR by ensuring regulatory and legal adherence. One example of such a regulation is the EU Network and Information Systems Regulations (NISR), which provide legal measures (covered by D7.7) aimed at enhancing the overall security, encompassing cyber and physical aspects of information and network systems. Such systems play a crucial role in facilitating the accessibility of digital services ranging from data processing to data storage in the cloud. The growing importance of the internet and information systems as crucial facilitators of societal and economic development justifies the implementation of this measure.

2.1.5. Cybersecurity and Infrastructure Security Agency (CISA)

As the sector-specific agency, the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS) collaborated with the Critical Manufacturing Sector Coordinating Council (SCC) to develop a sector-specific implementation guide centered on the manufacturing industry [8]. In line with NIST, CISA also provides a regulatory framework for information and cyber security guidance by evaluating and improving the ability of manufacturing industries to detect, prevent, and react to cyberattacks. It provides a high-level notion of risk management through the prioritize, orient, determine, analyze, and action plan concepts. The guide is a tool for harmonizing strategic operations and technological solutions for handling cybersecurity risks. It can be used to determine the most effective steps to mitigate a cyber threat. Organizations, industries, and businesses are just a few of the different categories of entities that can use the framework for various objectives.

The recommendations in the above-mentioned guides and standards are high-level, which might not be applicable to low-level systems, because no low-level system-specific information is included. To derive efficient security principles, it is essential to acquire thorough system understanding and analyze these recommendations within the context of this knowledge. In addition, substantial effort is required to verify these recommendations using structured tools, including the conversion of high-level suggestions into low-level security regulations and the design of such regulations for the

security evaluation. Moreover, many of the proposed measures ought to have been proposed and implemented for large industries because they are beyond the user's control. Also, since the privacy threats related to the sharing of data in IIoT are already addressed in deliverable D7.8, the focus of our guideline will therefore be primarily on detection and prevention/mitigation.

2.2. *Survey of Guides and Research Works in Academics*

2.2.1. General Surveys, Guides, and Research Works

Despite reviewing various cybersecurity frameworks and guide recommendations from the perspective of organizations, it is crucial to also investigate academic works and see what they have to offer. This would provide us with an overview of the most effective security measures for the IOP tools and infrastructure.

Given that most scholars acknowledge the fact that the majority of cyberattacks instigated against industrial systems lack preventive measures in place, it is crucial that preventive measures are considered prior to detection in the IOP infrastructure. This will greatly help to minimize the likelihood of an attack. Some notable state-of-the-works in the literature that fulfil both the preventive and detective criterion includes following works:

In [9], Bravos et al. provide a detailed analysis of two tangible instances of connected IIoT systems in smart factory and smart logistics environment, emphasizing the architectural decisions made to bolster cybersecurity measures. In addition, they include an interconnected industrial system that ensures safe data transmission and employs strategies for detecting and mitigating threats to both real-world data and IoT devices. Although the system is not readily available as a commercial product, its architectural design and outcomes demonstrate the benefits of employing advanced technologies like deep learning for threat detection and blockchain for improved communication within IIoT systems, specifically for the purpose of threat prevention. This analysis also explores the practical implementation of these technologies. The researchers ultimately presented the empirical findings pertaining to the different components of their system in the manufacturing domain, along with an evaluation of the overall system performance.

Since the authors place significant emphasis on the independence and portability of various components within their system, the majority of these components may be readily modified and used as independent services within other systems. Also, the suggested architectural framework has the potential to be used in other emerging IIoT systems with little to moderate technical adjustments. Therefore, the findings of their study may serve as a baseline reference for future studies in this domain.

Mahesh et al. [10] conducts an analysis and evaluation of the cybersecurity vulnerabilities within the evolving digital manufacturing environment. They evaluate the potential threats based on different case study scenarios and consequences for the manufacturing sector and proposes effective strategies to safeguard manufacturing operations. In terms of attack prevention, the authors emphasize on the possibility that not all participants in a manufacturing industry have the same level of resources to implement the most sophisticated defenses, because the vulnerabilities inside for instance, a supply chain, in addition to jeopardizing their own resources, have the potential to compromise the assets of every party involved in the supply chain. Therefore, while their primary emphasis in the research was on the cybersecurity measures used in the manufacture of distinct components within a Digital Supply-chain Network (DSN), they also acknowledged the significance of other components within the DSN, including the information, financial, and commercial networks. Finally, they also suggest certain methods to be adopted to ensure threat mitigation, such as established information security techniques like data encryption, watermarking, and authentication.

In [11], the authors aimed to provide educational resources to those without specialized knowledge on the safe deployment of IoT devices. To accomplish this, a compilation of effective guides and methodologies has been furnished, derived from established frameworks. The execution of these security measures was shown in two distinct situations, using a range of network devices and taking into account the limits often encountered by SMEs. They also conducted an evaluation of the current vulnerabilities that exist in smart devices as well as the existing standards pertaining to the safe deployment of Internet of Things (IoT) devices. Next, they proceed to execute the prevailing optimal strategies for ensuring the security of interconnected network devices, with a specific emphasis on preventive measure to the issues posed by the IoT. Lastly, they laid the groundwork for presenting a pragmatic framework that facilitates the secure deployment of IoT devices within SMEs.

Recently, Mekala et al. [12] provided an extensive review of the Industrial Internet of Things (IIoT) framework by identifying distinct sectors in which IIoT adoption occurs, an evaluation of potential risks and vulnerabilities, and an in-depth analysis of countermeasures that are currently available. The authors also highlight some preventive measures based on the integration of different technologies such as edge, blockchain, and advanced artificial intelligence, including deep learning, machine learning, and big-data analytics, while bringing forth some future challenges that can be mitigated by such technologies, including maintaining scalability in the IIoT, effective resource management approaches that facilitate data transfer without modifying the computational storage capacity of the sensors, heterogeneity and diversity of IIoT applications and protocols, IIoT architecture design flaws, and mapping industrial applications against the threat environment.

According to [13], the plethora of security challenges faced by IoT require not just detective measures, but prevention should be at the forefront of mitigating cyberattacks. Therefore, the authors outlined several security needs that have been suggested for the IoT while providing a thorough categorization of the primary security concerns pertaining to the architecture of the IoT, taking into account the potential consequences of attacks and other emerging security concerns. Moreover, they systematically compile and visually represent the many countermeasures used to address these vulnerabilities, while considering recent advancements in security methodologies. In conclusion, an in-depth evaluation of the specified countermeasures for IoT security is undertaken.

2.2.2. Blockchain-based Surveys and Research Works

Other works encourage the use of blockchain for secure smart factories; these include Elmamy et al. [14], Leng et al. [15], Rathee et al. [16], Maleh et al. [17], Pourrahmani et al. [18], Leng et al. [19], Nutter et al. [20], and Gimenez-Aguilar [21]. In [15], the authors examine the potential of blockchain systems for addressing cybersecurity challenges that may hinder the realization of intelligence in Industry 4.0. In this context, a total of eight cybersecurity concerns have been discovered within the realm of industrial systems. The authors then created ten comprehensive metrics via a scrutiny of existing research on blockchain-secured smart manufacturing, with the aim of facilitating the implementation of blockchain applications in the production sector. They provide valuable insights that will guide future research directions in the field of blockchain-secured smart manufacturing which can possibly drive research efforts to address important cybersecurity challenges in order to achieve intelligence in the context of Industry 4.0. Even with full trust in blockchain for ensuring the required protection against cyber threats, it still comes with its own fair share of vulnerabilities [22] such as the insertion of invalid transactions into a block, goldfinder, double spending, and wallet theft [22].

In another profound work by Nutter et al. [20], the authors identify major aspects of blockchain-based solutions in numerous sectors of Industry 4.0. In addition, they provided a framework that proved valuable in conceptualizing the integration of Industry 4.0 enabling technologies with blockchain technology, thereby facilitating the implementation of adept and effective blockchain-

based solutions within the context of Industry 4.0. In conclusion, using the suggested framework, the authors propose a hypothesis about the progression of blockchain technology in Industry 4.0 environments while emphasizing the pertinent areas of study that scholars and professionals engaged in this domain should focus on in the immediate future.

In a rather unexpected approach, instead of focusing on proposing solutions and mitigation strategies against cyber threats, Rainmundo et al. [23] debate on security surrounding the current topics in IIoT. The authors argue that due to the need for decision-making, cybersecurity must initially concentrate on the diverse vulnerabilities of IoT components before proceeding to work on its security mechanisms, such as access control, data storage, authorization, and privacy. While enterprises must adopt a cybersecurity plan with respect to their protection needs, emphasizing that organizations must stay abreast of technological advancements in order to respond appropriately to cybersecurity threats. In a nutshell, this all boils down to the fact that cyber security experts must be alert to the plethora of future challenges regarding cyber threats, while organizations must first look into preventive measures against cyber-attacks.

2.2.3. Chapter Summary

This section provides a summary of conclusions derived from this chapter in relation to the crucial security measures adopted for the benefit of the entire IOP tools and infrastructure. Below, we itemize our take from these surveys, both in academia and industry organizations.

Summary of Surveys from Organizations

1) To ensure IIoT security, the majority of the guides emphasize adopting proactive security measures before detection (reactive) measures. As such, our guides also embrace this strategy, thereby making sure that proactive measures are taken into consideration for the security and privacy of the IOP.
2) Amongst the guides, ENISA and CISA can be applicable to organizations, industries, and businesses, depending on the framework scope and its various objectives. Therefore, IOP security can derive advantages from the defined frameworks in these guidelines.
3) With the exception of ENISA and ETSI, other guides, especially NIST and ISO/IEC, are high-level, requiring an in-depth understanding of the infrastructure in order to analyze the measures within the context of the standards provided. Consequently, they might not be applicable to low-level industries.
4) ETSI is mainly concerned with the consumer aspect of the IIoT and focuses on European regulations. Its primary objective is to establish an initial framework for secure and efficient production within the context of consumer IoT. As such, some important future benefits can be derived for the consumer side of the use cases in the entire project.
5) Most of the guides and regulations also provide a general overview of frameworks that can be used to determine the most effective steps to mitigate a cyber threat.

Summary of Survey works from Academia

1) Fortunately, academia also places greater emphasis on proactive measures for ensuring IIoT security in the manufacturing industries prior to detection measures.
2) With the recent advances in deep learning and blockchain technologies, some of the works emphasizes the use of these advanced technologies for threat detection (via deep learning) and improved communication within IIoT systems (via blockchain). The adoption of such novel technologies shall be considered within the IOP depending on the security, performance, and scalability tradeoffs.
3) In addition to ensuring the security of digital services, networks, data, the cloud, etc., some researchers emphasize adopting the right architectural framework in order to enhance the

cybersecurity of the industry since the architecture encapsulates how services can be managed and how the network can be segmented, monitored, and mapped. This testifies to the need for adopting the right architecture for the IOP.

4) For a more efficient integration of cybersecurity measures, independent implementation of each component within the IIoT is also encouraged. So do our guides for securing the entire IOP.
5) Other works emphasize that each component within the infrastructure should possess the same level of resources to implement attack defenses because vulnerabilities within one component, such as a network, can lead to the compromise of other components, such as databases and devices. This is also captured in our guides.
6) Most research also stresses the potential of blockchain-based systems for addressing cybersecurity challenges that may impede the realization of intelligence in Industry 4.0. However, since the sole adoption of blockchain also comes with its fair share of vulnerabilities, ensuring a balance with other technologies is key for the optimal protection of the entire IOP.

3. Attacks and Protection Mechanisms

3.1. *Vulnerable Attacks in the IOP Tools and Infrastructure*

Before delving into the protection mechanisms that would be used to ensure the security of the IOP, it is important to briefly highlight some attacks that the IOP can be susceptible to. This will give an insight to the systems administrators on what to look out for and how to identify and differentiate between various attacks. In essence, this section should serve as an awareness raiser for the IOP system administrators on the various IIoT-related attacks to keep an eye on. For a more in-depth description and analysis of these attacks, readers can refer to the works in [3], [12], and [24]. While not all IIoT-related attacks mentioned in the refered documents can exploit the IOP, the predominant ones in the manufacturing domain relevant to our use cases include DDos, phishing, malware injection/ransomware, spoofing, man-in-the-middle, data sniffing and manipulation, and attacks targeting legacy systems. A brief description of these attacks is given as follows.

- **DDoS:** Distributed Denial of Service (DoS) attacks impede the flow of services to authorized users. The attacker engages in malicious operations that weaken the computational capacity of systems, rendering them inaccessible or overburdened by inundating the machines with a substantial influx of queries [12]. This attack can be used to target different parts of the IOP tools and applications, such as routers, network devices, servers, etc.

- **Man-in-the-middle attacks:** In this attack, the adversary attempts to interfere with or compromise the transmission of information between authorized entities, such as users, tools, and systems. In addition, the adversary may seek to modify the data prior to its dissemination to other entities. This attack can mainly target the communication channels between the IOP tools and applications through eavesdropping on messages, sniffing and spoofing of network channels, hijacking a session, etc., thereby taking control of tools within the architecture.

- **Malware injection:** In malware injection, or ransomware, the attacker deploys malware in an attempt to duplicate and transmit harmful code throughout the network, which might be appended to a trojan application to facilitate effortless infiltration into the system or architecture [12]. The primary objective of these attacks is to inject encryption techniques to encrypt the data or files of a targeted person or organization, with the intention of demanding a ransom in exchange for the decryption key. This attack is very detrimental as it can compromise the entire IOP data, communication channels, as well as I/O devices.

- **Phishing:** In phishing, the adversary assumes the identity of a legitimate user and deceives other authorized individuals within the organization into providing their private details on a bogus webpage or persuades them into downloading and installing harmful attachments such as viruses and malware, thus leading to the subsequent disclosure of sensitive data. This attack mainly targets sensitive information, such as login passwords, biometric identity, usernames, and secret credentials. A highly mutant variant of this attack is the spear phishing, where the attackers use specific social engineering content to target a specific organization.

- **Spoofing:** A spoofing attack involves an individual imitating the identity of a genuine user in order to deceive others and gain unauthorized access to a system, hence enabling the delivery of a malicious payload. By using methods such as IP spoofing, the adversary is able to manipulate the source IP address associated with the sent packets to deliver an exploit. A variant of such attack is also available in biometric systems, where the attacker uses a fake biometric template to fool the system in order to gain access.

- **Data sniffing and manipulation:** Sniffing and manipulation are all attack variants that can expose the confidentiality and integrity of the IOP systems. Such attacks make it easier to sniff or manipulate data in the transmission channels through eavesdropping and replay. It is often easier to perform these attacks on unencrypted data or communication channels that aren't secure.

Generally, the IIoT systems are considered some of the most vulnerable systems targeted by cyberattacks in both the IT and OT realms due to their heterogeneous interconnectivity; as such, the security of IT and OT play a crucial role in protecting the critical interconnected manufacturing systems against such attacks. Fig. 1 depicts the general taxonomy of IIoT attacks based on attack vector, attack target, attack impact, and attack consequences in both physical (OT) and cyber (IT) scenarios [12].

A comprehensive grasp of this attack taxonomy will help facilitate the secure and robust implementation of defenses within the entire IOP, thereby proactively recognizing and mitigating threats while safeguarding essential tools and critical infrastructure from unauthorized breaches.

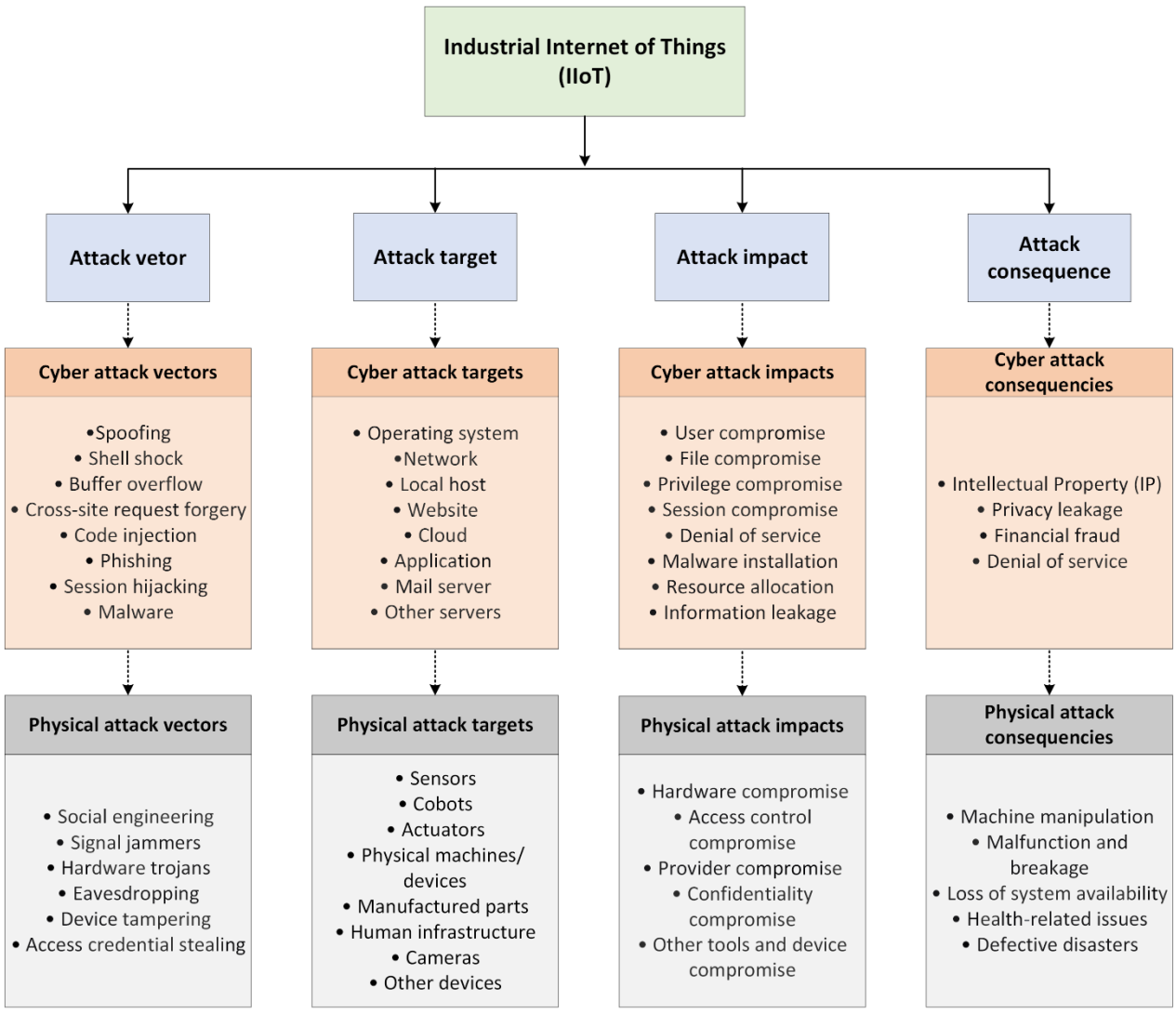

Figure 1. Attack taxonomy of the IIoT [24]

3.2. *Protection Mechanisms for the IOP Tools and Infrastructure*

In an era where the digital ecosystem is growing exponentially, the imperative to safeguard platforms and tools cannot be stressed enough. The IOP Tools and Infrastructure, recognising this imperative, places a pronounced emphasis on orchestrating robust protection mechanisms. This section delves into the multi-faceted layers of security and protection measures that will be developed to defend the platform's infrastructure, data, and users against the attacks discussed in section 3.1.

The landscape of protection is vast, and it requires a meticulous approach to ensure that no facet is left unguarded. Whether it's controlling access to physical and virtual resources, real-time monitoring for anomalies, or ensuring that data is handled with the utmost integrity and care, each dimension has its significance.

The subsequent sections from 3.2.1 to 3.2.5 provide a comprehensive look into the platform's commitment to security. The role-based access controls delineate clear boundaries, ensuring that only authorised personnel interact with critical infrastructure components. Real-time monitoring mechanisms provide a vigilant eye on system health and performance, ensuring swift responses to potential threats or failures. Moreover, with data being a cornerstone of the digital age, a set of strategies is presented, aimed at safeguarding it from various risks, whether they be unauthorised access, loss, or non-compliance with regulatory standards.

As the technological realm continues to evolve, so do the threats and challenges. This chapter, thus, stands as a testament to the IOP Tools and Infrastructure's unwavering commitment to staying ahead of potential risks and ensuring an environment where users can operate with trust and confidence.

3.2.1. Access Control (role-based)

In the modern digital landscape, ensuring secure, selective access to critical infrastructure is paramount. Uncontrolled or poorly regulated access can compromise the stability, security, and performance of a system, leading not just to operational hitches but also potential data breaches. With the Integrated Operations Platform (IOP) Tools and Infrastructure playing such a pivotal role in processing and safeguarding vast quantities of data, the adoption of a well-structured, role-based access control becomes non-negotiable. This section elucidates the tiered access control mechanisms that have been meticulously crafted for different components of the infrastructure.

The role-based access control (RBAC) framework employed here divides access into three distinct levels:

- Bare-Metal Servers: The foundational hardware layer that demands the highest security clearance given its significance in the overall system.
- Kubernetes API: Serving as the bridge between hardware and the services running atop them, the Kubernetes API has its own unique set of access prerequisites.
- Services in Kubernetes: These represent the myriad internal services such as Kafka and Druid, each with its own critical function within the system.

Each of these levels, with its specific access requirements and challenges, will be discussed in the following subsections. This hierarchical, role-based strategy ensures not only security but also optimizes system performance, making certain that every interaction is purposeful and authorized.

3.2.1.1. Access to Bare-Metal Servers

Ensuring the sanctity and security of the core infrastructure is paramount to the seamless operation and protection of the IOP Tools and Infrastructure. Within this sphere, controlling and regulating

access to bare-metal servers emerges as a foundational step. The strategies implemented for access control at this level comprise:

- Exclusive SSH Access for System Administrators:

Access to the physical servers via Secure Shell (SSH) is restricted exclusively to system administrators. By limiting this access, risks associated with potential breaches, misconfigurations, and unintended changes are significantly reduced. System administrators are equipped with the knowledge and skills to manage and maintain the infrastructure, ensuring that it runs efficiently without any compromise on security.

- Non-public SSH Access via VPN:

Public access to SSH is inherently risky, making servers vulnerable to a myriad of potential security threats. To mitigate these risks, SSH access has been configured to be non-publicly accessible. Instead, access is channelled through a Virtual Private Network (VPN). VPNs provide an encrypted tunnel for transmitting data, ensuring that any communication between the system administrator and the server remains confidential and secure from external threats. This measure not only enhances the security of data transmission but also reduces the potential attack surface by keeping SSH endpoints shielded from the broader internet.

By implementing these control measures, the IOP Tools and Infrastructure are robustly guarded against external threats at the foundational level. These practices ensure that only individuals with the requisite permissions and expertise can interact with the physical servers, thus preserving the integrity and security of the entire system.

3.2.1.2. Access to Kubernetes API

The Kubernetes API serves as the gateway to the orchestration and management of containerised applications within the infrastructure. Given its critical role, appropriate access controls have been instituted to prevent unauthorised interactions and maintain the system's reliability and security.

- System Administrators as Sole Interactors:

The Kubernetes API is reserved primarily for system administrators. This restriction ensures that only those with a comprehensive understanding of the system's intricacies and potential vulnerabilities can make changes or access data. By limiting access to this knowledgeable group, the risk of inadvertent misconfigurations, which could expose the system to security threats, is minimised.

- Abstraction of Kubernetes from Developers:

To further fortify the system, Kubernetes has been abstracted entirely from developers. Such a decision ensures that developers are shielded from the complexities and potential pitfalls of direct interaction with Kubernetes. Instead, they can focus on their primary task of developing and deploying applications without getting bogged down by infrastructural concerns.

- Controlled Interaction through CI/CD Pipelines:

Developers are not left entirely out of the loop. They can still interact with Kubernetes, but this interaction is carefully mediated through Continuous Integration/Continuous Deployment (CI/CD) pipelines. CI/CD pipelines automate the processes of application development, testing, and deployment, ensuring that changes are consistent, reproducible, and in line with established best practices. By funnelling developer interactions through these pipelines, the system guarantees that all changes to the infrastructure are controlled, deliberate, and free from common errors that could compromise security.

By instituting these access controls for the Kubernetes API, the IOP Tools and Infrastructure benefit from a balance between security and functionality. While the potential attack surface is minimised, developers are still empowered to perform their tasks efficiently, leveraging the power of Kubernetes indirectly.

3.2.1.3. Access to Services in Kubernetes

Within the Kubernetes infrastructure, several services, notably Kafka and Druid, play pivotal roles in processing, storing, and streaming vast amounts of data. Access to these services is of paramount importance for the smooth functioning of the system, and as such, has been meticulously controlled to ensure system security and data integrity.

- Isolation from External Access:

Services within the Kubernetes cluster, including but not limited to Kafka and Druid, are shielded from the outside world. This design decision eliminates the risk of external threats and unauthorised access attempts. By keeping these services internal, only platform-approved services and applications can communicate with them.

- Access Limited to Internal Platform Services:

Instead of a broad range of access points, the internal services in the Kubernetes cluster can only be accessed by specific, designated internal platform services. This streamlined approach to access means that even if an unauthorised entity were to somehow gain entrance to the platform, their ability to interact with these critical services would be significantly hampered.

- Benefits of Internal Restriction:

Restricting access in this manner comes with numerous benefits:

  - Security: By limiting the entities that can communicate with these services, the chances of a security breach or data leakage are considerably reduced.
  - Performance: A reduced number of interactions, especially from non-essential services, ensures that the system's resources are optimally used. This results in better response times and higher system availability.
  - Maintainability: With fewer points of interaction, system administrators can more easily monitor, manage, and maintain these services, ensuring their longevity and reliability.

In summary, the access controls placed on services within the Kubernetes infrastructure are not just about security, though that is a primary concern. They also play a vital role in ensuring the system's overall efficiency, reliability, and maintainability. This strategy aligns with the overarching goal of creating a robust, scalable, and secure IOP Tools and Infrastructure.

3.2.2. Real-time Monitoring and Incidence Response

Monitoring system health and responding to incidents in real time are indispensable for maintaining the optimal performance and security of any robust infrastructure. To address these needs in the Integrated Operations Platform (IOP) Tools and Infrastructure, a state-of-the-art monitoring and incidence response mechanism will be implemented.

The choice of monitoring tools plays a crucial role in the overall effectiveness of a system's monitoring capabilities. For this project, the Prometheus and Grafana monitoring stack will be selected. Prometheus, an open-source system monitoring and alerting toolkit, will be used for its powerful data scraping, storing, and querying capabilities. It will enable the collection of real-time metrics from various parts of the system, thus aiding in early detection of issues.

Complementing Prometheus, Grafana will offer advanced visualization features. It will serve as the user interface where administrators can view, analyze, and set up alerts on the metrics collected by Prometheus. This integration will enable a more user-friendly, effective way to monitor a complex system in real-time.

To ensure proactive response to system abnormalities, AlertManager will be incorporated. If a service or node becomes unhealthy or unavailable, AlertManager will trigger alarms, notifying the system administrators. This will facilitate quick, informed decision-making and actions, minimizing the impact and duration of any outages or system failures.

Together, these tools will provide a comprehensive real-time monitoring and incidence response solution, allowing for agile reactions to fluctuations in system health and ensuring continuous, secure, and efficient operation of the IOP Tools and Infrastructure.

3.2.3. Data Security

In the digital realm, data stands as the bedrock upon which platforms and services are built. Ensuring the utmost security of this data is not just a necessity but a duty, considering the significant value and sensitivity it holds for individuals and organisations alike. The sections that follow within the 3.2.3 framework detail the rigorous steps and measures that will be developed for the IOP Tools and Infrastructure to ensure the safety, security, and compliance of data at every juncture.

From access controls that employ sophisticated authentication mechanisms to backup strategies ensuring swift recovery in adversity, each facet of data handling is approached with meticulous care. The platform recognises the multilayered challenges of data security and responds by instituting a comprehensive system to address them. Whether it's preventing potential leaks, auditing usage, or ensuring compliance with ever-evolving data protection regulations, the IOP Tools and Infrastructure is committed to upholding the highest standards.

In the subsequent subsections, a detailed examination is provided on how the platform will handle essential elements of data security, such as Data Access Control, Data Protection and Backup, Data Usage Audit, Data Leak Prevention, and Data Compliance. Each of these aspects plays a critical role in creating a cohesive and resilient data security framework that aims to protect stakeholders at every turn.

3.2.3.1. Data Access Control (via Queries)

In the digital era, the safeguarding of data access is paramount. With escalating cyber threats and sophisticated infiltration methods, the manner in which data is accessed and utilised has never been more under scrutiny. Within the Integrated Operations Platform (IOP) Tools and Infrastructure, a rigorous data access control system will be established, primarily channelled through queries.

A pivotal element of this strategy will be the implementation of a robust authentication and authorization mechanism on the serving layer. This will ensure that only legitimate requests are processed, significantly reducing the risk of malicious data breaches. While the specific details of this mechanism will be further defined as the project progresses, the initial inclination is towards leveraging token-based systems, with JWT (JSON Web Tokens) being a probable choice.

JWT offers a compact, URL-safe means of representing claims between parties. When employed as an access token, it can be used to determine what resources the token bearer can access. The advantages of JWT include its self-contained nature, as it carries all necessary information, reducing the need for repeated database lookups. Furthermore, its stateless and scalable nature aligns well with the IOP's operational objectives.

The objective is to make data access not only secure but also streamlined and efficient. The mechanism will distinguish between different user roles, ensuring that each user can only access the data pertinent to their responsibilities and within their privilege levels. This will be pivotal in minimising internal data breaches or unintentional leaks.

By rigorously controlling data access via queries and employing cutting-edge token-based systems, the IOP Tools and Infrastructure will aim to stand as a paragon of data security and operational efficiency.

3.2.3.2. Data Protection and Backup

The reliability and integrity of data storage systems are of utmost importance for any advanced digital platform. Ensuring the protection of this data, both against potential external threats and systemic failures, remains a paramount objective for the IOP Tools and Infrastructure.

To uphold data protection standards, a rigorous encryption technology strategy will be employed. Through this, all stored data will be securely protected against unauthorized access attempts. This encryption will act as a solid barrier, preventing any unauthorized entities from interpreting or misusing the data, even if they were to gain access to the storage systems.

Alongside data encryption, it's also imperative to consider potential data losses that might arise from systemic failures, errors, or unforeseen events. To address these concerns, regular backups of all data will be implemented. These backups are designed to ensure a quick and efficient restoration process, minimising potential downtime or service disruptions. The backup systems will be strategically distributed, guaranteeing redundancy and ensuring that a single point of failure does not compromise the data's availability.

By combining state-of-the-art encryption technologies with a comprehensive backup plan, the IOP Tools and Infrastructure will be positioned to always maintain data integrity and availability. Such protective measures are crucial for retaining user trust, ensuring operational continuity, and complying with industry standards and regulations.

3.2.3.3. Data Usage Audit

Understanding how and to what extent data is utilised within the IOP Tools and Infrastructure is essential for a myriad of reasons, ranging from optimising system performance to ensuring compliance with data protection regulations. Implementing a systematic approach to auditing data usage provides insights into the operational dynamics and potential areas for enhancement.

The monitoring stack, comprising Prometheus and Grafana, will be pivotal in this data usage audit process. This combination offers a robust mechanism to capture a wide array of metrics related to data usage, including volume, frequency, and type of data requests. These insights can aid in identifying trends, spotting anomalies, and diagnosing potential issues that may arise in real-time.

Moreover, understanding data access patterns can offer valuable intelligence about system utilisation, highlighting areas that might benefit from further optimisation or additional resources. Furthermore, such audits can help ensure that access patterns align with stipulated guidelines, detecting any anomalous or unauthorised access that might indicate a breach or misuse.

In conclusion, the data usage audit system that will be developed for the IOP Tools and Infrastructure will not only bolster security but also provide the insights necessary to maintain an efficient and highly responsive platform.

3.2.3.4. Data Leak Prevention

Ensuring the confidentiality and integrity of data is paramount, especially in an era where breaches can result in significant financial and reputational damage. Data leaks can originate from various sources, be it inadvertent mistakes, system vulnerabilities, or malicious attacks. Therefore, a holistic approach to data leak prevention is indispensable to the IOP Tools and Infrastructure.

One of the primary mechanisms to counteract potential data breaches will be the encryption of all communications into and out of the platform using the Transport Layer Security (TLS) protocol. TLS ensures that data in transit is protected from eavesdropping, tampering, or forgery, thus creating a secure communication channel between the user and the platform.

Additionally, measures will be developed to monitor and detect unusual activity patterns, which might suggest potential leaks. Any anomalous activity will trigger alerts, facilitating rapid intervention and containment. These mechanisms, combined with a robust logging system, will offer traceability and allow for timely forensic investigations should any breach occur.

Furthermore, regular security assessments and penetration testing will be conducted to identify and rectify vulnerabilities proactively. By employing a combination of preventative measures and responsive strategies, the IOP Tools and Infrastructure aims to uphold the highest standards of data protection, ensuring that users can trust the platform with their data, confident in its security and resilience.

3.2.3.5. Data Compliance

In the rapidly evolving landscape of digital platforms, compliance with data protection laws and regulations is not only a legal obligation but a demonstration of the platform's commitment to the responsible and ethical handling of user data. The IOP Tools and Infrastructure places great emphasis on staying abreast of changes in legislation and regulatory requirements, ensuring that the platform remains compliant at all times.

Ongoing surveillance of legislative changes is crucial as data protection laws can vary by jurisdiction and are frequently updated to address new challenges and technologies. This constant vigilance ensures that the platform's practices and policies align with the latest standards, including those set by the General Data Protection Regulation (GDPR) and other relevant regional and international statutes.

Moreover, the platform will undergo periodic audits to ensure that all data-handling practices are up to the mark. These audits, conducted by internal or external parties, assess the effectiveness of implemented policies and practices, highlighting any areas that might require improvement.

Training and awareness campaigns will also be initiated for staff and stakeholders, ensuring that everyone involved understands their roles and responsibilities when it comes to data protection. This is particularly important as human error is a significant factor in many data breaches.

In essence, the commitment to data compliance in the IOP Tools and Infrastructure is multifaceted. It entails proactive measures to stay updated with the legal landscape, regular audits to ensure adherence, and continuous education of all involved parties. Through these measures, the platform will remain a trusted and reliable entity for all users and stakeholders. Table 1 depicts the IOP protection mechanisms and the attacks they'll mitigate.

Table 1. Summary of the IOP protection mechanisms and attacks they protect against.

Protection mechanisms	Attacks mitigated in the IOP
Authentication	*Spear phishing, spoofing, keyloggers, credential stuffing, brute force, and man-in-the-middle attacks.*
Access Control (role-based)	*Spoofing, phishing, eavesdropping, keyloggers, brute force, and credential stuffing.*
Monitoring and Incidence response	*Spyware, signal jammers, device tampering, hardware trojans, social engineering, and credential stealing.*
Data access control (via queries)	*Malware injection, data sniffing, replay, spoofing, man-in-the-middle attacks.*
Data protection and backup	*Malware injection, man-in-the-middle, data manipulation, ransomware, data sniffing.*
Data usage audit	*Data sniffing, data manipulation*
Data leak	*Data sniffing, data manipulation, leak prevention.*
Data compliance	*Data manipulation*
Network security	*DDoS, IP spoofing, signal jammers, phishing, buffer overflow*

3.2.4. Authentication

In the open-source IOP, a robust authentication system is paramount to ensure that access is granted only to authorised entities. Single Sign-On (SSO) will be a key feature in the architecture of the IOP's authentication system. With SSO, users will be able to securely access multiple applications or services within the IOP ecosystem using a single set of credentials, streamlining the login process without compromising security.

3.2.4.1. Verification and/or Identification

The IOP's authentication is bolstered by a rigorous verification and identification process. Users will be required to confirm their identity through a secure, multifaceted method, thereby enhancing the security landscape. The incorporation of mechanisms like two-factor authentication or biometric verification in conjunction with SSO will ensure a fortified security perimeter.

As users attempt to access various services, the IOP will efficiently authenticate and validate their credentials, balancing between security and user convenience. Unauthorized access attempts will be identified and mitigated, thanks to real-time monitoring and adaptive authentication protocols that adjust based on the perceived level of risk.

3.2.5. Network Security

Network security within the IOP will be a blend of advanced technologies and protocols, engineered to ensure the integrity, confidentiality, and availability of data. A meticulously configured firewall will be instrumental, established to scrutinise and manage the traffic based on an organisation's predetermined security rules, acting as the first line of defence against potential cyber threats.

The IOP will employ TLS (Transport Layer Security) to encrypt communication channels, ensuring that data exchanged between users and the platform, or within the platform's internal communications, remains confidential and tamper-proof. This layer of security will be fundamental in safeguarding sensitive information and maintaining users' trust.

Administrative access to the platform will be strictly regulated and highly secure. Admin access will be facilitated through a dedicated VPN (Virtual Private Network). This approach will ensure that administrative interactions with the platform are secure, encrypted, and isolated from potential

external threats. The VPN will not only facilitate secure access but will also ensure the confidentiality and integrity of the administrative communications.

Moreover, the network security strategy will incorporate continuous monitoring, anomaly detection, and instant response mechanisms to promptly address any emerging threats. By utilising machine learning and AI, the IOP's network security will be adaptive, learning from ongoing traffic patterns to identify and mitigate potential threats proactively.

In essence, the integration of a firewall setup, TLS encryption, and admin access through a dedicated VPN is designed to fortify the IOP's network security, offering a resilient, secure, and efficient environment for users and administrators alike.

4. Guide to a Secure and Open-Source AI-Based IOP Infrastructure

This section provides the guidelines for achieving secure and open-source AI-based IOP in ONE4ALL. The guidelines use the best security measures for mitigating cyberattacks, taking into account the digital services, modules, and other IoT devices in the IOP network. Thus, ensuring that the protection mechanisms highlighted in Section 3 above are observed and implemented according to protocols that will be itemized and explained in this chapter. It is worth nothing that the guidelines are in accordance with the most recent and stringent criteria defined by the European Commission and other relevant regulatory authorities.

4.1. *Guide to Secure Digital Services and Modules*

4.1.1. Authentication

For the vast majority of systems and networks, authentication is the first layer of protection. Prior to accessing the network, tools and applications should be verified with the goal of eliminating malicious devices from the IOP ecosystem, thus preventing the infiltration and dissemination of falsified data. Authentication mitigates a variety of attacks, including phishing, keyloggers, credential stuffing, brute force, and man-in-the-middle attacks, among others. Guidelines to be considered for the IOP authentication include.

1. Modify default system settings: As a first measure, the default credentials that come with all the IOP tools and system applications should be modified. System administrators and users should, by all means, avoid running devices with default credentials.

2. Avoid using the same logins: Additionally, system administrators and users should avoid reusing the same credentials across multiple devices. If the authentication mechanism is a password, at least three letters should be modified to some arbitrary random word that the user can remember. If it's a hardware token, a new one should be generated, and if it's a biometric, a biometric template protection mechanism should be incorporated into the authentication system such that an old template can be revoked and replaced by a new one in the event of an attack.

3. Ensure device credentials are not hard-coded: Following the reset of a password or token, it is essential to disable the functionality of the default login. However, if the system is still functional on such default logins, it is possible that the credentials have been hard-coded. In such a scenario, it is advisable to replace the device or opt for an alternative product.

4. Adopt a good authentication mechanism: A soundproof authentication mechanism(s) should be adopted. More preferably, two factor authentication such as biometrics and one-time password/hardware token should be given utmost consideration.

5. Frequent password update: If by any means system administrators and users decide to use a password/token for access, a frequent password and token update policy should be adopted by the administrators. It can be quarterly or in every three months interval.

6. Ensure default hardware reset devices are protected: Furthermore, ensure that any hardware reset procedures on all IOP devices are password-, token-, or biometrics-secured, protected, and difficult to access, as they can revert to the default device factory settings.

4.1.2. Access Control

Access Control is another crucial protection mechanism for the IOP that allows permissions and privileges to various tools and system applications within the IOP. Thanks to the hard-coded role-based access control framework based on bare-metal servers, the Kubernetes API and other services in Kubernetes, including Kafka and Druid, that will all be integrated in the IOP. Also, more layers of security will be ensured within the IOP in terms of access controls, given that access to the physical servers via SSH is restricted exclusively to system administrators, and SSH access has been configured to be non-publicly accessible. Instead, access will be channeled through a VPN, thereby ensuring that any communication between the system administrator and the server remains confidential and secure. All these prove the provision for a strong access control mechanism in the IOP. However, other measures that should be adhered to by the administrators include the following:

1) Define roles: To start, it is necessary to identify the various functions existing within the IOP structure. When creating these roles, it is important to take into account the job duties, responsibilities, and access needs associated with them.

2) Define permissions within the IOP structure: Permissions may be defined as the precise authorizations that are necessary for each position. This entails the identification of the specific tasks and operations that users in each position should possess the capability of executing. This should be applied to all tools and devices within the entire IOP infrastructure.

3) Role's allocation within the IOP: This task involves the allocation of certain roles to particular users, with the criteria for these assignments being determined by their respective work positions and associated obligations. It is paramount to ensure that each user is appropriately assigned to the role(s) that accurately represent their access needs.

4) Mapping roles within the IOP: Role mapping involves the establishment of connections between roles and permissions. The allocation of permissions to certain roles is essential to ensuring that users assigned to a given position are granted the appropriate access privileges. System administrators should be careful while establishing such connections to avoid granting privileges to unauthorized users or the other way around.

5) Periodic evaluations and updates: It is important to conduct regular evaluations in order to ascertain that role assignments and permissions are consistently matched with any changes that may occur within the IOP framework or the entire manufacturing industry at large. Ensure that the appropriate modifications are made to accommodate newly assigned responsibilities or to make necessary adjustments to existing roles as required.

4.1.3. Data Security/Encryption

Data encryption is a process that involves the transformation of data into a coded form, therefore ensuring its confidentiality and integrity, even in the event of illegal interception of the encrypted data packets during transmission. This approach demonstrates a high level of efficacy in safeguarding data and guaranteeing its integrity in the face of potential security breaches. In order to ensure the security of data of the IOP and its services, a rigorous encryption technique and data backup procedures will be implemented. Thus, ensuring unauthorized access to the data, and efficient data restoration in the event of unforeseen system failures or data loss.

In terms of data access, the IOP will provide a robust authorization mechanism in the serving layer by leveraging token-based systems built on JWT (JSON Web Tokens), thereby offering a compact, URL-

safe means of representing claims between parties while ensuring secure and efficient data access. All these testifies that data in the entire infrastructure is well secured both in transit and at rest. However, other important measures that should be observed to enhance data security between the IOP and its digital services and modules includes the following.

1) Pay attention to sensitive data: Given that the IOP will deal with a lot of data in transit, which is regarded as very sensitive compared to data at rest, it is crucial that administrators use the chosen strong encryption techniques to safeguard any sensitive data before transferring it. Also, ensure the use of encrypted protocols such as HTTPS, SSL, TLS, FTPS, and others to guarantee the protection of data during transit.
   Meanwhile, to ensure the security of data at rest, it is recommended to use encryption techniques to encrypt important files before their storage or, alternatively, by opting for the encryption of the storage device itself.

2) Ensure a secure network connection: To enhance the security of data during transmission in addition to encryption, it is essential to deploy robust network security measures such as firewalls and network access control mechanisms. These network security solutions play a crucial role in safeguarding data transmission networks from potential threats posed by virus or other unauthorized invasions.

3) Use preventive security measures: To ensure precautionary measures on important data for the entire IOP infrastructure, it is not advisable to depend only on reactive security techniques for the protection of important data. Rather, it is recommended to use proactive security techniques that can detect data that is at risk and execute efficient data protection protocols for both data in transit, data in use, and data at rest. Some of these proactive measures include routine security calibrations on all data transmission channels, devices, and modules.

4) Ensure user prompts for sensitive data: Select secure data solutions that include rules and privileges allowing for user prompting, blocking, or automated encryption of sensitive data throughout its transmission. This includes scenarios where files have been attached to email messages, transferred to cloud storage, detachable drives, or any other form of data transfer.

5) Establish a data categorization policy: It is important to establish policies that provide an organized strategy for categorizing and classifying all data within the infrastructure, regardless of its location. This will guarantee that suitable measures for data security are consistently implemented when the data is in a static state and that appropriate actions are taken when data identified as vulnerable is accessed, used, or transmitted.

6) Ensure the use of a trusted, secure, and reliable cloud vendor: When considering the use of a public, private, or hybrid cloud provider for the purpose of data or application storage, it is imperative to conduct a thorough evaluation of cloud vendors with regards to the security measures they provide. However, it is crucial to note that relying only on the cloud service for data protection is not advisable. Inquiries about the entities with data access, the encryption methods used, and the frequency of data backups are crucial to address.

7) Ensure the right trade-off balance between security and performance: The security and performance conundrum is a general challenge that exists in all security domains, and this is even a more serious issue in data security. Whenever an encryption technique is applied to data, it is always possible to experience a reduction in the performance of such data, depending on the system and purpose it is applied to. Therefore, it is crucial that the right

protection mechanism be selected for specific data, as this will reduce the impact of such a trade-off.

4.1.4. Tools and Device Management

The IOP tools and devices are a huge part of the entire infrastructure, and similar to data, it is essential to ensure that they are also secured from cyber threats. Even though the project has adopted the implementation of monitoring tools such as Prometheus and Grafana, it is worth noting that these tools are essentially used for the collection of real-time metrics from various system sources in order to ensure the early detection of system errors and other unforeseen issues. Therefore, as a preventive measure, we deem it paramount to propose some guidelines to be followed on the tools and devices that will be used in the entire ONE4ALL.

1) Use devices with encryption capability: Ensure that all devices within the IOP infrastructure can be encrypted. In the event that a device lacks functionality for an encrypted communication channel through wireless connectivity, it is advisable to establish a wired connection instead. Also, if a device lacks the capability to provide encryption, it is advisable to acquire an alternative device or entirely disconnect the device from the network infrastructure.

2) Ensure correct configurations: Misconfiguration flaws during device security settings are often overlooked in manufacturing industries, which can be detrimental to the entire infrastructure. It is essential that developers, system administrators, and employees pay close attention to the security configurations of any devices that would be used within the IOP infrastructure. Ensure that you establish and monitor non-default security settings for devices, including the programs and applications running on them, while removing any unused features, programs, or applications.

3) Ensure frequent device updates: In addition to ensuring all devices are correctly configured, it is also crucial to set an automatic patch update on devices as soon as released. In the event of a delayed patch release, you must check for updates on a regular basis. Check the manufacturer's website for updates; if updates are no longer offered, consider purchasing a new device. Also, conduct frequent and periodic assessments and audits for missing or outdated patches and possible vulnerabilities in misconfigurations.

4) Ensure antivirus and firewalls are installed: When using IOP tools and devices, it is imperative to safeguard each device within the network, with special attention given to "legacy" laptops. This can be achieved by setting up firewalls and antivirus software on all laptops, desktops, and servers. Additionally, tablets and smartphones should be configured with proper security settings, such as two-step authentication, strong passcodes, restricting automatic Wi-Fi connections, and exercising caution when installing new applications.

5) Adopt factory reset if a malfunction is detected: If any tool or device connected to the IOP is noticed to exhibit decreased performance or malfunction, it is a sign of the presence of viruses. Certain types of computer viruses may be stored in the device's memory and can be effectively removed via the simple act of restarting the device. If the device continues to exhibit slowness or unresponsiveness even after a reboot, it is advisable to do a factory reset. Also, when excessive internet use or billing costs are noticed, this may indicate a potential hijack of a device. The adoption of a factory and passcode reset procedures should solve this issue.

6) Ensure adequate management of all tools and devices in the IOP: Attackers use various devices, including routers, switches, and endpoints, to get unauthorized access to industrial data and applications. They do this by exploiting vulnerable ports, excessively permissive network traffic rules, and hardware that has not been sufficiently patched or maintained. Therefore, it is essential to ensure that all these negligence are carefully mitigated during device and system installations and updates.

7) Ensure the removal of unused features: It is imperative that all features that are no longer needed within the IOP tools and applications be removed as soon as possible. Failure to eliminate unnecessary features and components exposes the application to vulnerabilities. This, in turn, creates an opportunity for attackers to exploit the application using techniques like code injection, whereby malicious code is inserted and then executed by the application.

4.2. *Guide to Secure Network Interconnectivity*

A secure network connectivity is considered pivotal to achieving profound protection in any security domain, let alone in cyber-security. Therefore, considering the interconnectivity nature of the IOP infrastructure, it is crucial to ensure that the network connection between the IOP and its modules is secured. This section provides guidelines on practical implementations that ensure the security of the entire IOP network interconnectivity.

4.2.1. Network segmentation

One of the crucial steps of securing heterogenous network connection is through network segmentation. Network segmentation refers to the procedure of partitioning expansive networks into smaller sub-networks in order to restrict traffic flow across various regions to prevent the spread of malwares. Such compartmentalization enables network administrators to effectively modify security regulations with enhanced accuracy. The implementation of such segmentation within the IOP will serve as a preventive measure for network attack mitigation while significantly contributing to the development of detailed security procedures and the establishment of security rules based on contextual factors.

Moreover, once the network has been partitioned, the process of establishing monitoring capabilities, identifying network inefficiencies, and improving its security is significantly facilitated. Therefore, it is important that the given network segmentation guidelines are adhered to within the entire IOP infrastructure.

1) Identify and classify asset values: Prior to initiating any network segmentation procedures, it is essential for the IOP to conduct an inventory of all components, such as databases, cobots, tools, devices, sensors, cameras, etc., and allocate corresponding values to them. It is important to arrange each item based on their respective levels of significance and sensitivity. These categorizations will afterwards serve the purpose of defining the different zones of trust within the IOP network.

2) Merge relevant network resources: After completing the documentation of different items, the next phase involves defining categories of similar network resources. Items with lower security levels should be consolidated within a single network, while those with higher security levels should be allocated to a separate network. As the network architecture takes shape, the IOP can implement enhanced security measures on networks containing more critical data in order to ensure protection.

3) Ensure the mapping of data flows throughout the network: Since network segmentation enhances network security by isolating network segments, the mapping of data flows across such segments makes it more difficult for an intruder to penetrate the network even after gaining an initial access. Hence, such mapping strategy should be adopted in the entire IOP to enhance the security of the network connection. However, it is important to do a comprehensive mapping of data flows across all systems inside the network, including the following:
    - *North-bound traffic:* The traffic that goes out of the IOP network. Such as employees using managed devices connected to the IOP network to access external domains.
    - *East-west traffic:* The traffic between systems within the network perimeter, such as a front-end webserver and a back-end database server in the IOP's data center network.
    - *South-bound traffic:* The traffic that consists of data entering a network segment, such as staffs or clients accessing the IOP's intranet web server.

4) Ensure the deployment of segmentation gateway: Establishing segment boundaries is essential not only for assuring network security for the infrastructure, but also for making well-informed decisions using the network traffic. To enforce access controls on each network segment in the entire IOP, a segment gateway must be deployed to guarantee that all network traffic entering and leaving the segment must pass through the gateway. As a consequence, the IOP may need multiple gateways to implement effective segmentation. However, considering the significance of such gateways in achieving the required network protection, IOP can utilize virtual firewall to cut down cost.

5) Ensure the segregation of IOP devices from the rest of the network: With the roll-out of IPv6, the scalability of IoT networks is practically limitless. Therefore, all devices connecting to the IOP must be isolated from the rest of the network to prevent direct access. The network engineers might require distinct network cabling and switches, or alternatively, private VLANs, to safeguard against attacks to logical networks of similar devices. Another possible approach is using a set of designated IP addresses or employing Network Address Translation (NAT) techniques to allow for the restriction and supervision of network traffic via the administrative interface. The adopted Prometheus and Grafana can be utilized for such monitoring while dedicated routers handle the restriction.

6) Beware of excessive or inadequate segmentation: When implementing network segmentation, it is prevalent to over segment into too many networks or under segment into too few networks. If each network segment is not properly managed, over-segmentation can force staffers to pass through multiple access points in order to gain access to data, causing workflow delays and constraining traffic flow, as well as increasing security risks. Meanwhile, under-segmenting a network can also be inefficient if there is too little distance between each system, because two or three segments of a single network would not provide the necessary level of security for network segmentation. In an ideal situation, there should be a balance between having sufficient resources to monitor and manage several networks without compromising security or employee productivity.

7) Adhere to the privilege of least principle: After the successful implementation of network segmentation, it is imperative that each network within the IOP adhere to the zero-trust model and the concept of least privilege. These practices entail restricting network access at all levels, necessitating that all entities inside the network boundaries, whether internal or external, undergo authentication and verification prior to being granted access to further segments of the network. With zero trust, the administrator can promptly detect and identify

any malicious actors or unauthorized entities trying to breach the networks, thus granting only authorized users the appropriate permission to access a specific network segment.

4.2.2. Network monitoring

Network monitoring plays an integral role in the IOP network by monitoring and assessing the performance and resilience of the network. The IOP network is assumed to include sensors or monitoring points strategically positioned at critical sites, such as servers, firewalls, routers, etc., inside the network infrastructure to effectively record real-time data. Such data is further analyzed and used for different purposes. Some important guidelines to be adhered to for efficient IOP network monitoring include the following:

1) Frequently monitor segmented networks: To order to maintain the integrity of the IOP network infrastructure, it is essential that segmentation procedures include ongoing monitoring of the network traffic and performance to mitigate any potential gaps or vulnerabilities. IOP network administrators should ensure regular network risk assessments and penetration testing. This plays a crucial role in the identification of security vulnerabilities that need prompt mitigation.

2) Adopt frequent auditing of segmented networks: Periodic network audits are of crucial significance as they provide the IOP infrastructure with the opportunity to reassess the efficacy of their existing security practices. Updates to the network segmentation plan may be necessary due to the introduction of new users, processes, operations, or industrial requirements over time. It is ideal to perform such audits on a yearly basis.

3) Ensure packet filtering: By monitoring incoming network traffic, the IOP can adopt techniques that mitigate attacks such as DoS. These techniques include filtering traffic originating from a particular IP address, imposing limitations on the number of packets that can be transferred from a single IP address, and redirecting or discarding packets from designated IP addresses before they can reach their intended destination.

4) Keep an eye on network devices: Despite the monitoring and auditing of the network itself, it is imperative to also monitor the network devices within the entire IOP infrastructure such as routers, switches, firewalls, load balancers, and wireless access points. The objective of monitoring these devices is to ensure that the network is operating effectively and performing to the expected standards while ensuring security. It also helps the network administrators proactively detect issues and take appropriate measures to maintain a reliable and secure network infrastructure. In the event that certain devices are not in use, consider switching them off or disconnecting them from the power source.

5) Monitor the baseline network behaviour: In order to proactively detect possible issues, it is essential for the IOP network administrator to possess an in-depth grasp of the network's baseline performance. By observing and analyzing network behaviour over an extended period, ranging from a few weeks to several months, network administrators can gain insights into the typical patterns and characteristics of network activity. This process enables administrators to establish a reference point for normal network behaviour, thus setting up threshold values for the purpose of generating alerts once there is a change in network activity.

6) Implement reports at each layer: Networks operate according to the OSI model, whereby every communication inside a network entails the transmission of data between systems

through many end points, devices, and connections. Every component inside the network plays a role in facilitating data transfer operations at certain levels. For instance, cables at the physical layer, IP addresses at the network layer, transport protocols at the transport layer, etc. The failure of a data connection can occur at any of these layers or even at multiple points. Therefore, it is essential for the IOP to utilize a monitoring system that allows different technologies to monitor at all network layers as well as various types of network devices that would facilitate problem detection and resolution, such that whenever an issue is detected, the monitoring system can easily pinpoint where the issue comes from.

7) Implement high reliability monitoring system with flexible failover: Most monitoring systems are installed within the monitored network. This expedites and improves the data collection from monitored devices. Nonetheless, if a problem occurs and the network fails, the monitoring system may also fail, rendering all the collected monitoring data inaccessible or unusable for analysis. Therefore, it is encouraged that the IOP implement a monitoring strategy with high reliability without failover. High reliability and availability assure that the monitoring system does not have a single point of failure; therefore, even if the entire network goes down, the monitoring system is still accessible, allowing the network engineer to detect and resolve issues.

4.2.3. Network configurations

Similar to network monitoring, the importance of having the right network configurations for the IOP infrastructure cannot be over emphasized, as network configuration is essential for the industry's operations, IT efficiency, and connectivity while sustaining network traffic, assuring security, eliminating disruptions, and maintaining stability. While network monitoring focuses on collecting and analyzing data on network functionality and performance, network configurations proactively focus on configuring and managing network devices and services. Important guidelines that must be followed for efficient IOP network configuration are as follows.

1) In-depth understanding of the network architecture: First, a comprehensive knowledge of the IOP's network architecture and configuration, as well as the interconnected devices and their functional integration, is required. Additionally, it's crucial to have a complete inventory of all network equipment, including servers, firewalls, routers, and switches, as well as a network map that fully describes the software, hardware, systems, and devices present in the network. All these will give profound insight to the network engineers on how to better approach performance and security for the network infrastructure.

2) Ensure standardized configuration of devices: To mitigate the risk of human error or other configuration problems during the installation of new devices, it is advisable to establish standardized settings for each category of device inside the IOP network. This includes routers, switches, network topology, and other relevant components. By implementing such standardized configurations, we can ensure consistency and minimize the likelihood of misconfigurations or other operational issues when deploying new devices. Network configuration management software is an effective method for achieving this objective.

3) Keep track of and record changes: It is advisable to monitor and record incidents of configuration modifications within the IOP network infrastructure while establishing a system of notifications to promptly warn relevant parties upon their occurrence. It is also crucial to follow up with comprehensive backups of all network modifications to facilitate subsequent inspection in the event of errors and to enable the restoration of earlier settings if deemed essential.

4) Automate where necessary: The automation of operations within the IOP network devices that would otherwise need human involvement has the potential to mitigate the occurrence of human errors, facilitate teams in managing repetitive tasks, oversee configuration changes across several devices, and ensure adherence to regulatory requirements.

5) Ensure redundancy in your structure: Regardless of the level of preparedness, network components have the potential to experience failures (due to security breaches or otherwise), resulting in a complete interruption of operations. It is essential to mitigate possible catastrophes by implementing redundancy within the IOP's network infrastructure, thereby ensuring the continuity of network operations in the event of device malfunction.

6) Ensure a centralized configuration management: It is highly likely that the IOP development might be allocated a significant portion of resources towards network management activities, a substantial proportion of which are characterized by manual execution and repetitive in nature. Therefore, the adoption of a centralized network management technique will result in significant time and cost savings.

   The use of integrated network management procedures and tools will enable the administrators to remotely update and configure hardware while also facilitating the total automation of several simple processes. Hence, ensuring that minor configuration errors that might lead to network downtime, data loss, and other security issues are mitigated [25].

4.3. *Guide to Secure Cloud Database*

With the wide adoption of smart devices in manufacturing domain, the accumulation of huge data has never been easy and so is the adoption of third-party cloud services for storing such data, which eventually comes with enormous security and privacy risks. Although these technologies provide notable benefits in terms of scalability and accessibility, they also present distinct security concerns that cannot be overlooked, as well as devastating consequences that must be effectively mitigated in order to safeguard sensitive data. Therefore, it is essential that the IOP's infrastructure cloud database remains secure.

4.3.1. Cloud database

Although the guidelines highlighted in sections 4.1.1, 4.1.2, and 4.1.3 comprise of relevant items that play critical role for securing the IOP cloud database, such as the network security tools for securing the communication channel between the cloud database and other services, the data security techniques for encrypting sensitive data in transit and at rest, strong authentication, and access control to the cloud database, etc. Other important specific guidelines not covered in the aforementioned sections include the following.

1) Ensure a limited access of IOP database to third-party cloud vendors: In case the IOP team decides to indulge in the services of any third-party cloud vendors, it is very important they understand that even after ensuring the use of a trusted, secure, and reliable cloud vendor (as highlighted under the guidelines of data security), it is also crucial to ensure that they have full access control of the database themselves rather than the cloud provider. By so doing, they can decide whether or not to grant any access to the provider, and if they do, it should only be limited to the requirements and the period of time the permission should last.

2) Ensure the frequent monitoring of database activities: Consistent monitoring of database activity is an essential element in understanding data operations with respect to user activity and system functionalities in order to identify abnormalities in the IOP database. Consequently, frequent monitoring facilitates the early detection of possible risks, hence allowing rapid response measures.

3) Ensure the frequent auditing of database activities: Auditing serves to document the activities undertaken by both systems and users, enabling a comprehensive investigation of any possible incidents. The combined practices of auditing and monitoring the IOP cloud database will offer a complete perspective on database activity and make a substantial contribution to enhancing its security.

4) Ensure frequent database software updates: As any database can be susceptible to cyber threats, so can the database software, since adversaries are continuously in search of vulnerabilities to leverage. Therefore, to ensure the security of the IOP cloud database, it is crucial to consistently update and apply patches where needed to the database software, especially in instances where the IOP team may choose to host their own database in a cloud environment or use a modified variant of a cloud-based database solution.

5) Ensure database servers are separated from other servers: In an event that the IOP decides to host its own database, it is important to database servers are situated on an entirely separate host from other servers meant for services such as web, applications, or networks. This will help to reduce the risk of unauthorized users gaining access to the IOP database.

6) Ensure authentication and access control are implemented on the IOP database servers: In line with the guidelines for data security, it is important to reiterate the importance of authentication and access control for not just the data itself but also the database storing the data, considering those protection techniques are the first crucial steps in ensuring secure access to cloud databases.

   The IOP should make sure that the principle of first privilege is strictly adhered to, such that access privileges are only permitted to those who require them and only to the extent required. While authentication should not only rely on the use of passwords but also a combination of different authentication techniques (multi-factor), e.g., password, token, and biometric).

In order to ensure strict follow-through and implementation of the guidelines covered in this section, different measures are being taken to make sure the procedures and security mechanisms are applied and understood throughout the project. Tables 2, 3, and 4 provide a summary of the outlined guidelines and completion indicative measures to be considered in the further course of the project.

Further, adaptable checklists will be drawn up as the project progresses to simplify the consideration and integration of the guidelines presented and ensure implementation. In addition, future meetings with project partners will further explain the guidelines presented here and provide the opportunity for reviewing the guides against any security threats according to the needs of ONE4ALL.

Table 2. Summary of guides to secure digital services and modules with completion indicators.

Guide to Secure Digital services and modules		Completion Indicators
Authentication	- Modify default system settings. - Avoid using same logins. - Ensure devices and credentials are not hard-coded. - Adopt a good authentication mechanism. - Frequent password update - Ensure default hardware reset devices are protected.	Multi-factor authentication is required to access systems within the entire IOP infrastructure.
Access control	- Define roles. - Define permissions within the IOP structure. - Role's allocation within the IOP - Mapping roles within the IOP - Periodic evaluations and updates	Permissions are granted to only authorized users and denied to unauthorized users within the entire IOP.
Data security	- Pay attention to sensitive data. - Ensure a secure network connection. - Use preventive security measures. - Ensure user prompts for sensitive data. - Establish a data categorization policy. - Ensure the use of a trusted, secure, and reliable cloud vendor. - Ensure the right trade-off balance between security and performance	Entire IOP data is secured against any form of cyber and physical threats.
Tools and device management	- Use devices with encryption capability. - Ensure correct configurations. - Ensure frequent device updates. - Ensure antivirus and firewalls are installed. - Adopt factory reset if a malfunction is detected. - Ensure adequate management of all tools and devices in the IOP. - Ensure the removal of unused features	Tools and devices within the entire IOP infrastructure are protected against cyber and physical attacks.

Table 3. Summary of guides to secure network interconnectivity with completion indicators.

Guide to Secure Network Interconnectivity		Completion Indicators
Network segmentation	- Identify and classify asset values. - Merge relevant network resources - Ensure the mapping of data flows throughout the network. - Ensure the deployment of segmentation gateway. - Ensure the segregation of IOP devices from the rest of the network. - Beware of excessive or inadequate segmentation - Adhere to the privilege of least principle	The entire IOP network is mapped and segmented between critical systems and devices.
Network monitoring	- Frequently monitor segmented networks - Adopt frequent auditing of segmented networks: - Ensure packet filtering. - Keep an eye on network devices. - Monitor the baseline network behaviour. - Implement reports at each layer. - Implement high reliability monitoring system with flexible failover	The entire segmented IOP network is monitored, and audits are recorded accordingly.
Network configurations	- In-depth understanding of the network architecture - Ensure standardized configuration of devices. - Keep track of and record changes - Automate where necessary. - Ensure redundancy in your structure. - Ensure a centralized configuration management	Entire IOP tools and device network configurations are standardized and centralized.

Table 4. Summary of guides to secure cloud databases with completion indicators.

Guide to Secure Cloud Database		Completion Indicators
Cloud database	- Ensure a limited access of IOP database to third-party cloud vendors. - Ensure the frequent monitoring of database activities. - Ensure the frequent auditing of database activities. - Ensure frequent database software updates. - Ensure database servers are separated from other servers. - Ensure authentication and access control are implemented on the IOP database servers	The IOP cloud database is fully protected. It is regularly monitored, and audits are recorded accordingly.

5. AI-Based Ethics for Open-Source IOP

The rapid proliferation of AI in contemporary digital solutions offers unmatched capabilities in handling complex datasets, pattern recognition, and decision-making. While these advances promise tremendous benefits, especially in the realm of open-source IOPs, they also usher in challenges that span across ethics, security, and privacy. Embracing AI for open-source IOPs necessitates a meticulous approach that ensures these systems are both powerful and principled.

Section 5.1 delves into the broad ethical considerations associated with AI integration. As AI's potential grows, so does its responsibility. Addressing the societal and moral implications of its deployment is as critical as harnessing its computational prowess.

In Sections 5.2 and 5.3, the focus narrows to address the pressing concerns of security and privacy. The intersection of AI and open-source platforms offers unique vulnerabilities, necessitating proactive and robust countermeasures to safeguard user data and maintain system integrity.

Lastly, Section 5.4 underscores the overarching goal: the journey towards a trustworthy AI. Beyond the technicalities, the section outlines the importance of establishing AI that resonates with societal values, legal parameters, and ethical norms, aiming to foster a harmonious coexistence between AI and its human counterparts.

In essence, this chapter seeks to provide a comprehensive roadmap for the ethical development and deployment of AI within open-source IOPs, ensuring that as we step into a more interconnected, AI-driven future, it is done with caution, responsibility, and an unwavering commitment to human-centric values.

5.1. *Ethical Considerations*

As artificial intelligence (AI) continues to grow and integrate into various sectors, the ethical challenges it brings to open-source IOPs cannot be overlooked. AI's ability to handle large amounts of data, identify patterns, and make real-time decisions highlights its promise in improving efficiency, accuracy, and cost-saving. However, these benefits come with potential risks, such as bias, discrimination, and unintended outcomes due to a lack of clear understanding of the data or algorithms used.

When AI tools are deployed, there's a chance they might overshadow human judgment, leading to results that might not align with ethical standards. This could include AI taking over jobs traditionally done by humans or making decisions without fully grasping the data's nuances. Therefore, it's crucial to approach AI with a balanced view, considering both its technological advantages and the ethical concerns it might raise.

It is essential that AI aligns with core ethical principles: respect for individual autonomy, ensuring no harm, promoting fairness, and being explainable. Every AI implementation, especially in open-source IOPs, should be evaluated against these principles. By doing so, trust in AI systems can be strengthened, creating a foundation where innovation and ethical considerations go hand in hand.

5.2. *Mitigating Security Concerns*

Security remains paramount when deploying AI in open-source IOPs. Given that AI systems can autonomously make decisions and potentially have access to a vast amount of data, there's a heightened risk of misuse, especially if malicious actors target these systems. Open-source platforms, while championing transparency and community-driven development, can be especially susceptible due to their open nature.

Several steps could be taken to address and mitigate these security concerns:

- Regular Security Audits: Periodic assessments will ensure that AI algorithms and associated software are free from vulnerabilities. These evaluations, done by security professionals, will ensure the AI tools are robust against potential threats.
- Continuous Monitoring: By actively observing the AI systems in real-time, unusual activities or potential breaches can be swiftly detected and addressed.
- Access Control: Strict protocols will be implemented to ensure that only authorised individuals can interact with the AI system, especially in crucial areas that could significantly impact the IOP's operation.
- Community Vigilance: Given the open-source nature of the platform, the broader community will be encouraged to report vulnerabilities or potential security concerns. This collective approach not only harnesses the expertise from a diverse set of contributors but also promotes a proactive culture of security.

By adopting these measures, the goal is to make AI integration into open-source IOPs not just beneficial but also secure, fostering trust and reliability.

5.3. *Mitigating Privacy Concerns*

In the age of digital transformation, privacy is a cornerstone of user trust, especially when integrating AI into open-source IOPs. AI systems can process vast amounts of data, often personal or sensitive in nature, making them a focal point for privacy concerns.

To safeguard user privacy and uphold trust, the following measures could be undertaken:

- Transparency and Consent: Users will be thoroughly informed about how their data will be used, and explicit consent will be sought. Transparent practices ensure users remain in control of their information.
- Data Storage and Retention: Strict guidelines will be set for how long data can be stored. Once data has fulfilled its purpose or surpassed its retention period, it will be securely deleted.
- Regular Privacy Impact Assessments (PIA): By periodically conducting PIAs, the potential privacy risks associated with AI operations can be identified and addressed proactively.
- Privacy by Design: From the very outset of AI tool development, privacy considerations will be ingrained into the system. This approach ensures that privacy is not just an afterthought but a foundational principle.

With these comprehensive privacy measures in place, the AI's integration into open-source IOPs aims to respect and protect user privacy, ensuring that technological advancements do not come at the cost of individual rights.

5.4. *Towards a Trustworthy AI*

Incorporating AI into open-source IOPs is not just a matter of technical precision; it's also about ensuring that these systems are reliable, fair, and align with societal values. Trustworthiness in AI is a journey, requiring consistent and rigorous checks, adjustments, and commitments to a set of guiding principles.

- Lawfulness: Every AI system integrated into open-source IOPs will be developed to strictly adhere to all relevant laws and regulations. This ensures that the AI not only functions optimally but does so within the boundaries of legal standards.

- Transparency: For users to trust AI, they must understand how it operates. Therefore, efforts will be made to make the AI's processes and decisions as transparent as possible, providing clear explanations for its outputs.
- Accountability: If something goes amiss, there needs to be clarity on who or what is responsible. An accountability framework will be established to pinpoint responsibility in the event of discrepancies or failures, ensuring timely rectification and lessons learned.
- Ethical Integrity: Adherence to ethical principles and values is paramount. This includes ensuring that the AI respects human autonomy, promotes fairness, prevents harm, and is explicative in its operations.
- Technical and Social Robustness: Beyond just being technically sound, the AI will be designed to be resilient against biases and errors, ensuring accurate outputs. Simultaneously, its design will account for social implications, making certain it enhances societal well-being.
- Continuous Learning and Improvement: Recognizing that the field of AI is dynamic, there will be mechanisms in place for continuous learning and adaptation. Regular feedback loops will be established, and the AI will be updated as new knowledge, techniques, or ethical considerations come to light.

In summary, the aim is to ensure that as AI is integrated into open-source IOPs, it is not just intelligent but also worthy of trust. The outlined principles and strategies strive to establish AI not just as a tool but as a responsible and beneficial partner in the digital landscape.

6. Conclusions and Next Steps

With the recent wide adoption of Industry 4.0 in the manufacturing domain, cyber threats are considered one of the main challenges impacting the smooth and hitch-free transitioning of industries. To overcome such a challenge, this report presents guidelines and protection mechanisms for secure and open-source IOP infrastructure in ONE4ALL. The deliverable revised other existing guides and regulations. It also covered potential attacks the IOP could be prone to and protection mechanisms against those attacks. Moreover, comprehensive guidelines for ensuring a secure IOP are proposed. AI ethical considerations for user privacy are also covered.

As Task T3.2 progresses with the deliverable, the 2nd deliverable (D3.3) will ensure the guides and protection mechanisms in this report are followed and implemented. The expectations from 2nd D3.3 include the following:

T3.2 Implementation of a Secure and Open-Source IOP Infrastructure (M30)

Expectations on secure digital services and modules:

1) Multi-factor authentication is used to access systems within the entire IOP infrastructure.
2) Permissions are granted to only authorized users and denied to unauthorized users within the entire IOP.
3) Entire IOP data is secured against any form of cyber and physical threat.
4) Tools and devices within the entire IOP infrastructure are protected against cyber and physical attacks.

Expectations on secure network interconnectivity:

1) The entire IOP network is mapped and segmented between critical systems and devices.
2) The entire segmented IOP network is monitored, and audits are recorded accordingly.
3) Entire IOP tools and device network configurations are standardized and centralized.

Expectations for a secure cloud database:

1) The IOP cloud database is fully protected. It is regularly monitored, and audits are recorded accordingly.

Activities:

Implementation activities for all expectations are covered in Sections 4 and 3.2 of this deliverable.

References and Resources

[1] M. Fagan, K. N. Megas, K. Scarfone, and M. Smith, "IoT Device Cybersecurity Capability Core Baseline," in "NIST," https://csrc.nist.gov/pubs/ir/8259/a/final, 2020. Accessed: Sep 2023.

[2] NIST, "The NIST Cybersecurity Framework 2.0," https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd, 2023. Accessed: Sep 2023.

[3] ENISA, "Baseline Security Recommendations for IoT," in "The Context of Critical Information Infrastructures," ENISA, 2017. Accessed: Sep 2023. [Online]. Available: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[4] ENISA, "Guidelines for Securing the Internet of Things," in "Secure supply chain for IoT," ENISA, 2020. Accessed: Sep 2023. [Online]. Available: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[5] ETSI, "Cyber Security for Consumer Internet of Things: Baseline Requirements ", https://www.etsi.org/technologies/consumer-iot-security, 2020. Accessed: Sep 2023. [Online]. Available: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[6] ETSI, "Guide to Cyber Security for Consumer Internet of Things," https://www.etsi.org/deliver/etsi_tr/103600_103699/103621/01.02.01_60/tr_103621v010201p.pdf, 2022. Accessed: Sep 2023.

[7] ISO/IEC, "Cybersecurity," in " IoT security and privacy — Guidelines," https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27400:ed-1:v1:en, 2022. Accessed: Sep 2022.

[8] CISA, "Critical Manufacturing Sector," in "Cybersecurity Framework Implementation Guidance," https://www.cisa.gov/resources-tools/resources/critical-manufacturing-sector-cybersecurity-framework-implementation, 2021. Accessed: Sep 2023.

[9] G. Bravos *et al.*, "Cybersecurity for Industrial Internet of Things: Architecture, Models and Lessons Learned," *IEEE Access*, vol. 10, pp. 124747-124765, 2022, doi: 10.1109/ACCESS.2022.3225074.

[10] P. Mahesh *et al.*, "A Survey of Cybersecurity of Digital Manufacturing," *Proceedings of the IEEE*, vol. 109, no. 4, pp. 495-516, 2021, doi: 10.1109/JPROC.2020.3032074.

[11] S. J. Ghazaani, M. Faulks, and S. Pournouri, "Secure Deployment of IOT Devices," in *Blockchain and Other Emerging Technologies for Digital Business Strategies*, H. Jahankhani, D. V. Kilpin, and S. Kendzierskyj Eds. Cham: Springer International Publishing, 2022, pp. 271-316.

[12] S. H. Mekala, Z. Baig, A. Anwar, and S. Zeadally, "Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions," *Computer Communications*, vol. 208, pp. 294-320, 2023/08/01/ 2023, doi: https://doi.org/10.1016/j.comcom.2023.06.020.

[13] D. Swessi and H. Idoudi, "A Survey on Internet-of-Things Security: Threats and Emerging Countermeasures," *Wireless Personal Communications*, vol. 124, no. 2, pp. 1557-1592, 2022/05/01 2022, doi: 10.1007/s11277-021-09420-0.

[14] S. B. ElMamy, H. Mrabet, H. Gharbi, A. Jemai, and D. Trentesaux, "A Survey on the Usage of Blockchain Technology for Cyber-Threats in the Context of Industry 4.0," *Sustainability*, vol. 12, no. 21, p. 9179, 2020. [Online]. Available: https://www.mdpi.com/2071-1050/12/21/9179.

[15] J. Leng *et al.*, "Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 237-252, 2021, doi: 10.1109/TSMC.2020.3040789.

[16] G. Rathee, C. A. Kerrache, and M. Lahby, "TrustBlkSys: A Trusted and Blockchained Cybersecure System for IIoT," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1592-1599, 2023, doi: 10.1109/TII.2022.3182984.

[17] Y. Maleh, S. Lakkineni, L. a. Tawalbeh, and A. A. AbdEl-Latif, "Blockchain for Cyber-Physical Systems: Challenges and Applications," in *Advances in Blockchain Technology for Cyber Physical Systems*, Y. Maleh, L. a. Tawalbeh, S. Motahhir, and A. S. Hafid Eds. Cham: Springer International Publishing, 2022, pp. 11-59.

[18] H. Pourrahmani, A. Yavarinasab, A. M. H. Monazzah, and J. Van herle, "A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain," *Internet of Things*, vol. 23, p. 100888, 2023/10/01/ 2023, doi: https://doi.org/10.1016/j.iot.2023.100888.

[19] J. Leng *et al.*, "Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: A survey," *Renewable and Sustainable Energy Reviews*, vol. 132, p. 110112, 2020/10/01/ 2020, doi: https://doi.org/10.1016/j.rser.2020.110112.

[20] M. M. Nuttah, P. Roma, G. Lo Nigro, and G. Perrone, "Understanding blockchain applications in Industry 4.0: From information technology to manufacturing and operations management," *Journal of Industrial Information Integration*, vol. 33, p. 100456, 2023/06/01/ 2023, doi: https://doi.org/10.1016/j.jii.2023.100456.

[21] M. Gimenez-Aguilar, J. M. de Fuentes, L. Gonzalez-Manzano, and D. Arroyo, "Achieving cybersecurity in blockchain-based systems: A survey," *Future Generation Computer Systems*, vol. 124, pp. 91-118, 2021/11/01/ 2021, doi: https://doi.org/10.1016/j.future.2021.05.007.

[22] H. Hasanova, U.-j. Baek, M.-g. Shin, K. Cho, and M.-S. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *International Journal of Network Management*, vol. 29, no. 2, p. e2060, 2019, doi: https://doi.org/10.1002/nem.2060.

[23] R. J. Raimundo and A. T. Rosário, "Cybersecurity in the Internet of Things in Industrial Management," *Applied Sciences*, vol. 12, no. 3, p. 1598, 2022. [Online]. Available: https://www.mdpi.com/2076-3417/12/3/1598.

[24] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures," in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, 23-24 Nov. 2018 2018, pp. 124-130, doi: 10.1109/GCWCN.2018.8668630.

[25] S. Watts. "Network Configuration Today: The Ultimate Guide." https://www.splunk.com/en_us/blog/learn/network-configuration.html (accessed September 15, 2023).