Modular Integrated Sustainable Datacenter

Joint Cybersecurity Needs and Acceptance Criteria Research Aimed at End-users and All Other Key Stakeholders

Deliverable D3.1

Deliverable: D3.1 (Joint Cybersecurity Needs and Acceptance Criteria Research Aimed at End-users and All Other Key Stakeholders)
Work-package: WP3 (Cybersecurity Edge)
Lead authors: Ramin Yazdani (NBIP), Simon Kuhn (NBIP)
Contributors: Mattijs Jonker (University of Twente), Anna Sperotto (University of Twente)
Due Date: 30/06/2025
Submission Date: 30/06/2025
Pages: 20
Version: 1.0
Type: Internal Report

MODULAR INTEGRATED SUSTAINABLE DATACENTER

Rijksdienst voor Ondernemend Nederland

8ra CLOUD-EDGE CONTINUUM

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

Table of Contents

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

1 Executive Summary

This deliverable outlines the cybersecurity requirements and acceptance criteria for a secure-by-design, sustainable federated edge data center infrastructure, to be developed in the scope of the Modular Integrated Sustainable Datacenters (MISD) project. This report specifically provides insights into stakeholder needs, regulatory constraints, and technical demands, setting the foundation for a secure and interoperable edge data center deployment.

This report is generated based on a literature review on edge cybersecurity challenges, threats and solutions, drawing on insights from over fifty academic publications, industry standards, best practices, and regulatory frameworks. We identify several stakeholders in this research report ranging from traditional cloud providers to end-users.

Drawing upon multiple observations reported in the literature underscores that, besides traditional requirements in existing networking paradigms, new requirements emerge in the federated edge-cloud ecosystem. For example, users need to gain control over their data and its locality. Additionally, due to the heterogeneity of the ecosystem, mutual trust between stakeholders needs to be addressed, e.g., based on a zero-trust architecture. Additionally, edge data centers are considered to be deployed in physically isolated environments in which physical security cannot be guaranteed to the level of one in traditional data centers. This requires mechanisms to be triggered to protect digital security in case of unauthorized physical access.

MODULAR INTEGRATED SUSTAINABLE DATACENTER
Rijksdienst voor Ondernemend Nederland
8ra CLOUD-EDGE CONTINUUM

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

2 Introduction

The transformation and paradigm shift of digital infrastructure from existing centralized cloud ecosystems toward distributed edge computing introduces new opportunities in terms of energy efficiency and performance. Additionally, such a deployment helps address the privacy and regulatory compliance issues raised by a centralized data handling model of traditional clouds by keeping data regional [1]. Nevertheless, it also comes with new cybersecurity risks and challenges. The heterogeneity of such a distributed and multi-provider environment makes trust between the involved entities a complex issue. This research report investigates the specific cybersecurity needs and requirements of various stakeholders in the context of a federated edge-cloud design. The key objectives of this report are:

O1: Identifying stakeholders involved in a federated edge-cloud continuum

O2: Defining cybersecurity requirements of the ecosystem to satisfy the requirements of the stakeholders

O3: Specifying architectural concepts that need to be considered to address cybersecurity requirements

In the remainder of this report, we refer to the prospective outcome of the MISD project as the *federated edge-cloud* ecosystem/continuum. The research methodology of this report is based on a literature review on edge cybersecurity threats and solutions, considering academic publications, industry standards, best practices, and regulatory frameworks. We focus on various edge computing deployments that have been extensively studied by academic researchers and/or have publicly available documentation including European Telecommunications Standards Institute (ETSI) Multi-access Edge Cloud (MEC) [2], 3GPP EDGEAPP [3], cloudlets [4, 5], Cisco fog computing [6], open fog consortium [7, 8], and Groupe Speciale Mobile Association (GSMA) Telco Edge Cloud [9, 10].

The remainder of this report is structured as follows. Section 3 lists and analyzes the stakeholders involved in a federated edge-cloud ecosystem. Section 4 elaborates on the hypothetical architecture of the system and its relevant design choices and security concepts. In Section 5, we elaborate on the security, privacy, and trust concerns of the edge-cloud continuum. Finally, Section 6 concludes the report and provides recommendations and next steps to be considered.

MODULAR INTEGRATED SUSTAINABLE DATACENTER
Rijksdienst voor Ondernemend Nederland
8ra CLOUD-EDGE CONTINUUM
This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

3 Stakeholder Analysis

Several stakeholders are involved in a federated edge cloud continuum, each with their own interests and requirements. These stakeholders play a crucial mutual role in realizing a secure-by-design edge-cloud ecosystem since any design choice needs to consider interoperability and usability among all stakeholders. Standardized and commonly deployed security protocols should be implemented to facilitate interoperability.

Different frameworks have defined stakeholders involved in a federated edge-cloud ecosystem, by focusing on the objective relevant to their own scenario. OpenFog includes silicon manufacturer, system manufacturer, system integrator, software manufacturer, and application developer as the set of stakeholders in their ecosystem. Alternatively, GSMA defines a different set of stakeholders, including enterprises, service providers, edge service providers, edge interconnect hub providers, middleware providers, independent software vendors and developers, server and storage vendors, and network operators [9].

We populate the list of typical stakeholders based on the existing research that elaborate on the stakeholders involved in an edge computing ecosystem [11, 12] and industry standards and frameworks [7,9,13] on similar edge computing solutions. This includes *end-users*, *infrastructure providers*, *service providers*, *network/telecom providers*, *hardware vendors*, and *regulatory entities*. Note that a stakeholder can have more than one role in this ecosystem. For example, cloud providers and telecommunication operators can simultaneously operate several edge data centers while providing certain applications and services.

3.1 End-users

The diversity of end-users in a federated edge-cloud scenario is similar to ones in a traditional cloud ecosystem, ranging from individuals to IoT network operators and enterprises. However, due to the performance and latency promises of edge computing, new end-users and applications can emerge. A major difference and a new requirement for end-users is that they need to be in control of their data locality (see Section 5.1.1) and keep their data regional [14].

Consider a use case where a customer identifies a specific edge data center in which to deploy their resources. Customers will select the edge data centers with the explicit reasoning of localizing virtual compute resources to their physical location. This could mean connecting to the edge data center via wireless access, fiber connectivity, as well as direct connection if the edge data center is located on the same premises. Measures need to exist to ensure that user data is processed and stored within the boundaries that they have intended.

Legacy (brown-field) end-user devices are going to be involved in a federated edge-cloud that might or might not be capable of adhering to the security requirements of the edge ecosystem. In order to solve this concern, we might need to rely on edge data center nodes to act as a security proxy for these devices [15].

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

3.2 Infrastructure Providers

3.2.1 Cloud Providers

The paradigm shift from centralized clouds to a federated edge-cloud does introduce certain challenges for cloud providers as stakeholders. However, these challenges should not be a big barrier for them, as cloud providers are already accustomed to operating in multi-cloud environments. For example, concepts such as a zero trust architecture (see Section 4.1) already exist within cloud environments (even if not widely used in practice).

Cloud providers in traditional setups were in complete charge of the control plane in a centralized manner. Having to deal with heterogeneous edge data centers dynamically joining the network introduces challenges in terms of authentication and authorization. Cloud providers need standardized authentication and authorization mechanisms to handle this challenge in a federated environment (see Section 4.4).

Additionally, remote attestation capability in edge nodes (see Section 4.3) is a dependency that cloud providers are going to rely on to be able to communicate securely with these physically exposed components of the system.

Cloud networks are positioned rather centrally and are in possession of ample computational resources [16, 17]. This makes them a suitable candidate to deploy infrastructure protection and network monitoring systems (see Section 5.2) that can merge feeds from many edge nodes, providing them a representative view of the threat horizon [18].

3.2.2 Edge Operators

Edge nodes are the main addition in the transition from existing digital infrastructure to a federated edge computing scenario. The proximity of edge nodes to end-users puts certain responsibilities on the shoulders of edge operators. First, edge nodes need to incorporate proxies to handle legacy (brown-field) devices that do not meet the cybersecurity requirements of a secure-by-design system. For example, these proxies would take over computationally heavy cryptographic processes that legacy devices are not able to adhere to.

Given that edge nodes are expected to be operating in physically unprotected environments, additional measures are required to ensure data and infrastructure security (see Section 5.3). This includes measures to ensure the integrity of edge nodes as well as secure processing and storage of user data. They must also deploy mechanisms needed to enforce data locality.

Edge nodes can also be seen as the first line of defense against external threats originating from IoT networks and legacy devices. This calls for a lightweight infrastructure protection and monitoring system to be deployed at the edge to mitigate cyber threats closer to their source. These monitoring components can further contribute to shared and collaborative incident response processes in higher tiers of the system (e.g., ones in regional data centers or a central AI/ML-based infrastructure protection node). Moreover, the distributed telemetry provided by edge nodes can be merged to form a complementary view, supporting coordinated defense mechanisms across the system.

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

3.2.3 Orchestration Providers

Orchestration providers (such as Kubernetes, OpenNebula, and OpenStack) offer platforms and tools to allow infrastructure providers expose their resources (e.g., compute, storage, and networking) to application and service providers in a way that abstracts management complexity. In a federated system where data and processes dynamically move across multiple domains, orchestration providers are responsible for supporting federated identity and access control (e.g., to manage resource sharing), and securely managing workload placement (to ensure compliance with data locality policies). Additionally, they are responsible for logical isolation of workloads in virtualized environments, which is of high importance for critical applications.

3.3 Service Providers

Service providers deliver applications, services, and platforms at cloud and edge data centers, acting as an intermediary between infrastructure providers and end-users. This places them in a sensitive position with regard to data security and trust. Similar to other stakeholders of a federated edge-cloud system, securing Application Programming Interfaces (APIs) using standardized authentication and authorization protocols is a requirement for service providers to contribute to the ultimate security of the system.

3.4 Network/Telecom Providers

Telecommunication providers own fixed and mobile access and core networks, connecting end-users, edge nodes, and clouds. They can play different roles in a federated edge-cloud. One of their main roles is to manage the access networks connecting end-users to edge data centers.

3.5 Hardware Vendors

Hardware vendors play a crucial role in the ultimate security of a federated edge-cloud system. The lack of trust due to the heterogeneity of the involved components is a concern that can be addressed to some extent using hardware-based security. For example, chip manufacturers providing Trusted Platform Module (TPM)-enabled hardware can mediate the attestation (see Section 4.3) of the computational environment integrity. Additionally, they are responsible for providing secure and verifiable firmware update mechanisms to mitigate vulnerabilities throughout the entire life-cycle of devices.

3.6 Regulatory Bodies and Law enforcement

3.6.1 Regulatory Bodies

Regulatory bodies are responsible for the establishment and enforcement of security frameworks, guidelines, and standards to ensure data privacy and security, fair competition, and consumer protection. Several regulatory bodies and frameworks are relevant in the context of a federated European edge-cloud ecosystem. General Data Protection Regulation

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

(GDPR) [19] outlines that storage and processing of personal data must be done only within compliant jurisdictions and grants users control over their data. This is relevant in the context of a federated edge cloud where users are supposed to be in control of the locality of their data. The GDPR also mandates the timely reporting of data breaches, which calls for having a solid security monitoring and management system.

Network and Information Systems Directive 2 (NIS2 Directive) [20] mandates compliance of sectors with high criticality, such as digital infrastructure, to requirements like regular risk assessments, ensuring supply chain security, and reporting of significant incidents, among others. The EU Cybersecurity Certification Scheme (EUCS) scheme developed by the European Union Agency for Cybersecurity (ENISA) [21] in accordance with the EU Cybersecurity Act (EU CSA) [22] is a certification scheme to standardize the security assurance level of cloud services. EUCS requires several security aspects such as identity and access management, supply chain life-cycle management, incident monitoring and response, physical security, data encryption in rest, transit and (ideally) in use. EU Cyber Resilience Act (CRA) [23] mandates that products with digital elements (such as software, hardware, and connected devices) will only be made available on the market if they meet certain cybersecurity requirements and that the cybersecurity is ensured throughout their whole life-cycle. The Radio Equipment Directive (RED) has been extended to include cybersecurity and privacy requirements [24], which is of relevance for wireless network operators to protect personal data and privacy of end-users, as well as preventing unauthorized access or transmission.

3.6.2 Law Enforcement

The concept of storing and processing data at the edge means that, in contrast to the traditional networks, end-user data no longer passes a core network. While preserving the privacy of the end-users, this introduces a limitation for Law Enforcement Agencies (LEAs), as it is not trivial to figure out where relevant data resides and who controls it [25, 26]. Additionally, malicious actors can obfuscate their activities by moving their resources between multiple edge nodes. On-demand synchronization of edge data to a central node under legal authorization can partially address this challenge. Using tamper-proof logging systems, such as distributed ledger-based logging, is another way to assist the traceability of network activities [27,28]. The infrastructure protection component (detailed in Section 5.2) can also partially contribute to this challenge by logging incidents in multiple hierarchical tiers.

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

4 Deployment Architecture and Concepts

The purpose of this section is to formulate a high-level picture of what the edge data center - based European Cloud can look like (inspired by the existing similar architectures [29, 30]), as well as outlining some of the key design concepts that are relevant to realize a secure-by-design federated edge-cloud. Figure 1 depicts a high-level view of major components involved in a federated edge-cloud and their connection. In the following, we briefly discuss two specific use cases that we have identified for this environment.

In the first use case, an end-user can identify a region (or a data center within a region) where they want their resources to be deployed. The regional data center operator can make a decision to deploy virtual resources in an edge data center, e.g., to take advantage of the energy efficiency offered by that edge data center. This use case is thus an extension of the user experience when deploying virtual resources within a traditional cloud provider environment.

In the second use case, the end-user can directly identify a specific edge data center in which they prefer to deploy their resources, e.g., with explicit reasoning of localizing virtual resources to their physical location. Thus, user resources cannot anymore be considered for migrations related to energy efficiency as it would violate the user's data locality requirements.

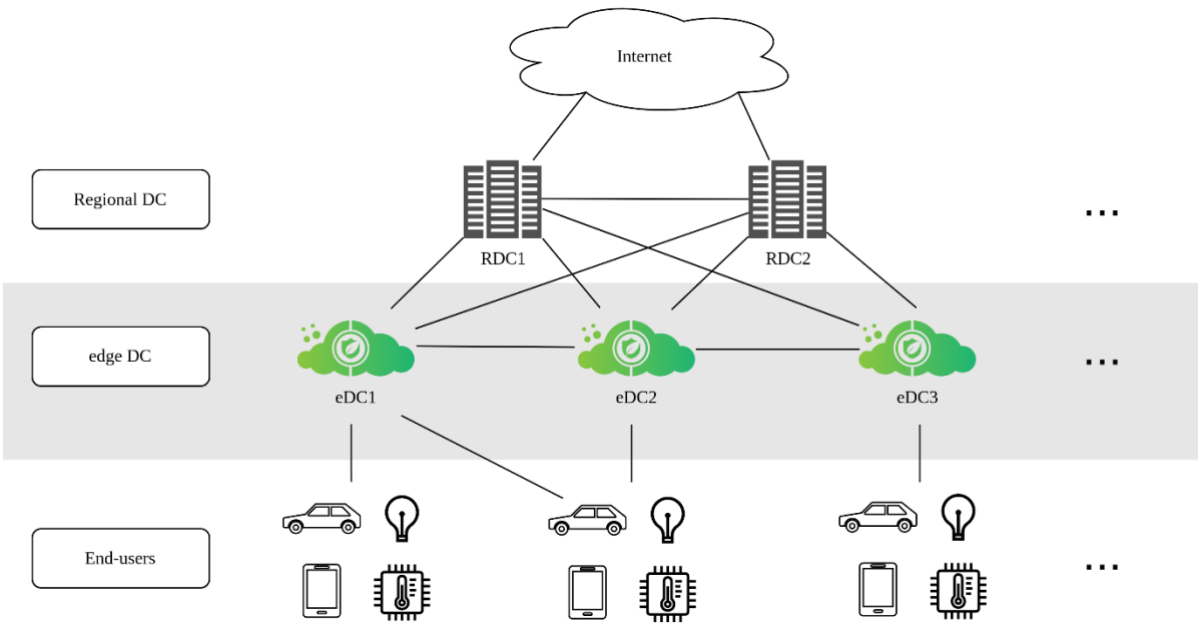

Figure 1: High-level architecture of a federated edge-cloud ecosystem. This diagram serves as a conceptual overview only. To ensure sustainability and resilience, different components of the system need to have redundant connectivity. For example, at the network level, multiple independent network paths should exist between different edge data centers, as well as between edge data centers and regional data centers.

The heterogeneity of the distributed edge data center ecosystem and the lack of an established trust calls for design choices that address its security issues, keeping in mind that

MODULAR INTEGRATED SUSTAINABLE DATACENTER
Rijksdienst voor Ondernemend Nederland
8ra CLOUD-EDGE CONTINUUM
This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

there is no central entity to be held liable if things go wrong. In the following, we elaborate on zero-trust, life-cycle management, attestation, and Identity and Access Management Services (IAMS) as some of the concepts that need to be taken into account to develop and implement a secure-by-design edge-cloud ecosystem. Note that these concepts are not mutually exclusive. For example, realizing a zero trust architecture relies on assessing the identity of users, which is done through Identity and Access Management Services.

4.1 Zero Trust Architecture

The heterogeneous nature of a federated edge-cloud ecosystem results in the lack of an implicit trust in comparison to the traditional centralized deployments. Security threats can originate both from within the ecosystem as well as from external networks. Thus, a secure-by-design implementation needs to be built with the Zero Trust [31] concept in mind replacing traditional perimeter-based network security, where any entity inside the network is considered to be trusted by default. A zero trust architecture focuses on resources, users, and assets in place of static network perimeter-based security principles. Additionally, users and devices might change their behavior over time, e.g., due to zero-day vulnerabilities or because of having been tampered with. Thus, they need to be re-verified continuously to maintain trust during their life-cycle. An orchestrator needs to periodically request attestation based on the deployed zero trust policies to assess the trustworthiness of the components (e.g., user, devices, and services). Nevertheless, security needs to be in balance with usability in the process to avoid motivating users to bypass security measures.

4.2 Supply-Chain Life-Cycle Management

Various components of the edge-cloud ecosystem that were trusted in the past might change their behavior over time. This can happen for many reasons. For example, the hardware of a node might have been compromised due to physical security limitations. The software running on a node can also be tampered with through malicious code injection (e.g., SolarWinds supply chain attack [32]). Bogus updates can also introduce vulnerabilities to systems (e.g., CrowdStrike incident [33]). This calls for a continuous auditing of the security for the components that form a federated edge-cloud continuum.

Software Bill of Materials (SBOM) [34] is one of the concepts that has recently gained attention for software development life-cycle and software supply chain risk management. SBOM provides a detailed list of components involved in a software, such as open source libraries, third-party code, version numbers, dependencies, links, and licensing details. Leveraging SBOM adds transparency to software supply chain management and facilitates incident response and compliance with regulations. Similarly, Hardware Bill of Materials (HBOM) [35] can be utilized for hardware supply chain risk management.

4.3 Attestation

Attestation refers to processes used to verify the trustworthiness of various elements of a system. Considering that federated edge-cloud devices and services are supposed to be

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

operated by different administrative domains, attestation is needed to ensure that code and data are only running in trusted environments and adhere to agreed-upon security policies. Attestation helps mitigate risks of physical attacks, which are not unexpected in a decentralized edge ecosystem.

Attestation is typically performed using hardware-based security modules – such as TPMs, and Trusted Execution Environments (TEEs) like Intel's Software Guard Extensions (SGX) and ARM TrustZone – in combination with remote attestation mechanisms.

4.4 Identity and Access Management Services (IAMS)

While IAMS is not a novel concept and it is a well-established process in traditional cloud networks, certain challenges emerge when putting it in the context of a federated edge-cloud continuum due to the distributed, decentralized, and heterogeneous nature of the system. Federated edge-cloud systems span multiple administrative domains and platforms, requiring dynamic trust relationships.

In such an ecosystem, identity and access management can be done similarly to a multi-cloud or hybrid cloud architecture, where a standalone vendor is used as an identity provider to decouple Identity and Access Management (IAM) from other services and provide flexibility in accessing resources. For federated access across all services and resources within Europe, a top tier could be identified based on central location, from which users and permissions can be defined by tenants. User permissions would then only be replicated to regions where resources are deployed for a given tenant. When resources for a tenant are deployed in a given region, Identity and Access Management Service profiles can be deployed to the service datastores within that region for rapid authentication and low latency. An alternative is to leverage federated identity management using solutions such as OpenID Connect (OIDC) [36].

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

5 Security, Privacy, and Trust in Federated Edge-Cloud

Several frameworks and definitions exist to model information security requirements. One of the widely referenced models is the CIA (Confidentiality, Integrity, and Availability) triad. Additionally, attributes such as privacy and trust are relevant in the context of a distributed edge-cloud ecosystem. Trust is a concern considering the heterogeneous nature of a federated edge-cloud ecosystem, and privacy needs to be highlighted as it is one of the key goals of such a deployment, promising to provide end-users with control and transparency over their data and its locality.

The OpenFog reference architecture [7] considers node security, network security, and management and orchestration security as its security requirements. Additionally, Martin et al. [8] consider physical security, end-to-end security, trustworthiness, and security monitoring and management as node-centric security aspects of an OpenFog system. We consider the following aspects relevant for the cybersecurity of a federated edge-cloud continuum without focusing on a specific component of the system, inspired by the existing standardization efforts [7] and academic research [8, 37, 38].

5.1 Data Privacy and Security

Data Privacy and data security are two foundational concepts that are largely intertwined. Several relevant aspects are detailed in the following.

5.1.1 Data Locality

One of the major promises of moving toward edge computing is providing end-users with control over the locality of their data. Keeping user data close to its source not only minimizes latency and increases the power consumption efficiency, but also reduces the risk of data exposure to unauthorized entities. Attribute-Based Access Control (ABAC) [39] is one of the concepts that can be leveraged to ensure context-aware processing of data in distributed and rapidly changing environments. For example, ABAC's environment attributes, such as time and location, can define where and when certain data can be stored, accessed, and processed.

5.1.2 End-to-End Security

End-to-end security is a crucial aspect to ensure data security that spans the entire life-cycle of data, from digestion to processing and storage. This means that data must be encrypted at rest (e.g., full disk encryption), in transit (e.g., using TLS protocol), and ideally while being processed (e.g., using homomorphic encryption [40]). In the context of a federated edge-cloud where trust across multiple administrative domains is a substantial challenge, mutual authentication mechanisms such as mTLS and federated identity, e.g., OAuth 2.0 [41] in conjunction with OIDC [36], can be leveraged to ensure end-to-end security and secure APIs.

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

5.1.3 Virtualization Security

Edge services heavily rely on virtual machines and containers [2]. Virtualized environments need to be secured against threats such as side-channel exploits. This is a bigger concern when considering critical applications and processes running on the edge that need a sufficient amount of resource isolation. While virtualization security is also an important aspect of traditional cloud security, federated edge computing introduces new challenges to addressing it.

Applications and workloads can move dynamically between multiple edge data centers, e.g., due to energy efficiency strategies, user mobility, or network conditions. This increases the complexity of workload isolation. Additionally, edge resources are considered to be heterogeneous, and their capabilities can be quite diverse. For example, certain edge nodes may not support hardware-based isolation (e.g., Intel SGX), limiting their security features.

5.1.4 Data Availability

In order to comply with EU regulations such as the NIS2 Directive, data availability needs to be ensured for business continuity and recovery from attacks such as ransomware. Measures such as redundant storage and regular backups can facilitate this goal. Implementing such measures not only facilitates regulatory compliance but also strengthens the trustworthiness and operational resilience of the entire federated edge computing ecosystem.

5.2 Network and Infrastructure Protection

Protecting IT infrastructure as one of the assets of a federated edge-cloud is essential to ensure resilience and availability of the ecosystem. This is not just a best practice but also a legal obligation mandated by EU cybersecurity regulation frameworks such as the NIS2 Directive.

Due to the distributed nature of the edge ecosystem, malicious traffic can flow into the network from multiple endpoints. Additionally, the security landscape is very dynamic, and new vulnerabilities can be introduced at any moment, leading to new attack vectors. This can make threat detection and mitigation challenging since every network element receives a partial view of the entire threat landscape. To address this, it is essential to deploy infrastructure protection in a multi-tiered and federated way. Doing so, malicious traffic can be blocked close to its source as far as possible, while highly distributed malicious traffic can be detected using aggregated intelligence from various nodes [7].

We envision a multi-tiered infrastructure threat detection and protection model, e.g., using signature-based detection and anomaly-based detection [42], deployed in different hierarchical levels of the system. Edge protection nodes can act as the first line of defense and stop malicious traffic from further navigating through the network. The advantage of leveraging this layer for infrastructure protection is that it can protect the rest of the infrastructure from malicious traffic originating from IoT devices that are generally considered to be less secure than the rest of the assets in the network. Additionally, this would ensure that upstream infrastructure resources are not wasted to handle malicious traffic, such

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

as Distributed Denial of Service (DDoS) attack traffic. Such a design can then also contribute to the sustainability of the federated edge-cloud ecosystem, which is one of the key features of the MISD project.

A second layer of protection can be implemented by collecting threat intelligence from edge protection nodes. This provides an insight into distributed security threats (e.g., DDoS attacks) that are likely not detectable by relying on a single edge data center.

Finally, a centralized AI/ML-based infrastructure protection system can exist to provide a long-term and representative view of the threat landscape by correlating telemetry data across different infrastructure protection nodes [30,43]. This is in line with a model considered for security monitoring and management of an OpenFog system [8], where security events are collected and aggregated in a Security Information and Event Management (SIEM) system in either a centralized or distributed manner and using both rule-based and behavioral analytics. Considering the requirements to ensure data locality, collaborative AI/ML models need to be trained to provide the intelligence needed for infrastructure monitoring and protection.

5.3 Physical Security

Edge nodes are considered to be deployed in physically isolated sites in which the physical security can not be guaranteed compared to the well-secured centralized data centers of traditional cloud providers. This introduces new challenges that need to be addressed to keep the end-to-end security and privacy of the ecosystem intact.

A secure-by-design implementation of edge nodes needs to consider this lack of physical security and treat devices as if they might already be tampered with. Physical platform security, using TPM [44] standardized by Trusted Computing Group (TCG) [45] as a root of trust, is one of the technologies that can be leveraged in this scenario. Additionally, virtual TPMs [46] can be leveraged to address the resource limitations of hardware-based TPMs. This is what OpenFog reference architecture also takes into account by stating that all fog nodes must implement a hardware-based immutable root of trust. Data needs to be encrypted in rest, transit, and (ideally) in use as encouraged by the ENISA EUCS scheme to avoid unauthorized access in case of a physical security breach. Infrastructure protection component can also be helpful here, where the protection system can enable detection, alerting, and immutable logging potential misuse.

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

6 Conclusions, Recommendations, and Next Steps

In this report, we outlined the cybersecurity requirements and acceptance criteria for a secure-by-design, sustainable federated edge data center infrastructure, focusing on three key objectives. We addressed our first objective (**O1**) by composing a set of stakeholders based on existing research, industry standards, and frameworks. Additionally, we elaborated on the cybersecurity of a federated edge-cloud (**O2**) by focusing on security, privacy, and trust to satisfy the requirements of the stakeholders involved in such an ecosystem. Finally, we highlighted several architectural concepts (**O3**) that need to be considered in the design of an edge-cloud continuum to ensure that cybersecurity requirements can be met.

In the following sections, we touch upon a set of recommendations and next steps towards realizing a secure-by-design federated edge-cloud.

6.1 Engaging with Similar Frameworks and Standardization Entities

Several working groups and entities have been pushing developments in the area of edge computing. There is quite some overlap between these efforts, their design principles, and security requirements with those of the MISD project. For example, ETSI, as a European institute already documented various aspects of a Multi-access Edge Cloud through ETSI ISG MEC. Another example is the OpenFog Consortium, where security is considered as one of the pillars of their architecture and documented. Considering the synergy and overlap of these systems, MISD can benefit from following developments within ETSI, OpenFog, and other similar projects in realizing a federated European edge-cloud ecosystem.

6.2 Post Quantum Security

As developments around quantum computing move forward, promising to solve complex computing problems, new concerns are raised regarding the resistance of current security standards and best practices against attacks using quantum computing power. Any solution for a future-proof distributed edge-cloud needs to be designed with the mindset of moving towards quantum-safe security, e.g., by leveraging Quantum Key Distribution (QKD) in combination with quantum-safe symmetric key cryptography, or using quantum-safe encryption algorithms such as code-based, hash-based, lattice-based, and multivariate cryptosystems [47–49].

Quantum-safe cryptography is not only needed when quantum computing is widely available. Timely integration of quantum-safe cryptography is crucial considering sensitive communications, such as the healthcare domain, that need long-term confidentiality. Data encrypted with traditional cryptographic algorithms (such as RSA) that lack Perfect Forward Secrecy (PFS) can be stored by adversaries to be decrypted in the future using quantum computing power.

MODULAR INTEGRATED SUSTAINABLE DATACENTER
Rijksdienst voor Ondernemend Nederland
8ra CLOUD-EDGE CONTINUUM
This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

Certain challenges need to be tackled in migrating toward quantum-safe cryptography. Quantum-safe cryptosystems feature significantly larger key sizes compared to traditional systems. This adds to the computational and communication overhead that might not be trivial considering the integration with existing infrastructure, e.g., edge devices (especially IoT devices connected to edge data centers) that are typically resource-constrained [47]. Additionally, establishing a QKD channel over long distances is challenging, considering rapid QKD signal degradation in fiber due to scattering and absorption. Finally, existing protocols such as TLS need to be modified to incorporate new ciphersuites. This usually comes with a long uptake time even after standardization [50].

6.3 Distributed Ledgers and Smart Contracts

The outline of realizing the federated edge-cloud is that there is not going to be a central entity to manage the security of the entire ecosystem. Distributed ledgers and smart contracts can be leveraged to implement distributed trust policies, identity and access management, and tamper-proof audit logs [51,52]. Considering the potentially low computational resources of edge devices (e.g., IoT devices) and applications requiring low latency, permissioned ledger platforms such as Hyperledger Fabric [53] are a promising option to consider.

Participants of a permissioned ledger are known to each other, and a certain level of trust exists in a way that they can develop legal agreements to handle incidents based on a governance model. Also, a permissioned ledger platform enables the privacy and confidentiality of transactions and smart contracts.

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

References

[1] J. Ortiz, P. J. Fernández, R. Sanchez-Iborra, J. B. Bernabe, J. Santa, and A. Skarmeta, "Enforcing GDPR regulation to vehicular 5G communications using edge virtual counterparts," in *2020 IEEE 3rd 5G World Forum (5GWF)*, pp. 121–126, IEEE, 2020.

[2] "Mobile-Edge Computing – Introductory Technical White Paper," tech. rep., European Telecommunications Standards Institute (ETSI), September 2014.

[3] "3GPP EDGEAPP." https://www.3gpp.org/technologies/edge-app, 2023.

[4] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The Case for VM-based Cloudlets in Mobile Computing," *IEEE pervasive Computing*, vol. 8, no. 4, pp. 14–23, 2009.

[5] M. Babar, M. S. Khan, F. Ali, M. Imran, and M. Shoaib, "Cloudlet Computing: Recent Advances, Taxonomy, and Challenges," *IEEE Access*, vol. 9, pp. 29609–29622, 2021.

[6] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog Computing and Its Role in the Internet of things," in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, pp. 13–16, 2012.

[7] OpenFog Consortium, "OpenFog Reference Architecture for Fog Computing." https://www.iiconsortium.org/pdf/OpenFog_Reference_Architecture_2_09_17.pdf, February 2017.

[8] B. A. Martin, F. Michaud, D. Banks, A. Mosenia, R. Zolfonoon, S. Irwan, S. Schrecker, and J. K. Zao, "OpenFog Security Requirements and Approaches," in *2017 IEEE Fog World Congress (FWC)*, pp. 1–6, IEEE, 2017.

[9] "Telco Edge Cloud: Edge Service Description and Commercial Principles," 2020. GSMA Whitepaper.

[10] "Operator Platform: Requirements and Architecture, Version 6.0," tech. rep., GSMA, February 2024.

[11] A. S. George, A. H. George, and T. Baskar, "Edge Computing and the Future of Cloud Computing: A Survey of Industry Perspectives and Predictions," *Partners Universal International Research Journal*, vol. 2, no. 2, pp. 19–44, 2023.

[12] R. Tourani, S. Srikanteswara, S. Misra, R. Chow, L. Yang, X. Liu, and Y. Zhang, "Democratizing the Edge: A Pervasive Edge Computing Framework," *arXiv preprint arXiv:2007.00641*, 2020.

[13] "MEC Security: Status of Standards Support and Future Evolutions," Tech. Rep. White Paper No. 46, European Telecommunications Standards Institute (ETSI), June 2023. Accessed: 2025-04-16.

[14] P. Garcia Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino, A. Iamnitchi, M. Barcellos, P. Felber, and E. Riviere, "Edge-centric Computing: Vision and Challenges," 2015.

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

[15] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, "EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4719–4732, 2018.

[16] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *Journal of Internet Services and Applications*, vol. 1, pp. 7–18, 2010.

[17] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," Special Publication SP 800-145, National Institute of Standards and Technology, 2011.

[18] J.-S. Shin and J. Kim, "SmartX Multi-Sec: A Visibility-Centric Multi-Tiered Security Framework for Multi-Site Cloud-Native Edge Clusters," *IEEE Access*, vol. 9, pp. 134208–134222, 2021.

[19] "General Data Protection Regulation (GDPR)." https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng, 2016.

[20] "NIS2 Directive: new rules on cybersecurity of network and information systems." https://digital-strategy.ec.europa.eu/en/policies/nis2-directive, December 2022.

[21] European Union Agency for Cybersecurity (ENISA), "European Cybersecurity Certification Scheme for Cloud Services (EUCS)," tech. rep., ENISA, 2020.

[22] European Union, "EU Cybersecurity Act." https://eur-lex.europa.eu/eli/reg/2019/881/oj, Apr. 2019.

[23] European Union, "EU Cyber Resilience Act." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847, Nov. 2024.

[24] European Commission, "Commission delegated regulation (eu) 2022/30 of 29 october 2021 supplementing directive 2014/53/eu of the european parliament and of the council with regard to the application of the essential requirements referred to in article 3(3), points (d), (e) and (f), of that directive."

[25] V. Prakash, A. Williams, L. Garg, C. Savaglio, and S. Bawa, "Cloud and Edge Computing-Based Computer Forensics: Challenges and Open Problems," *Electronics*, vol. 10, no. 11, 2021.

[26] M. Herman, M. Iorga, A. M. Salim, R. H. Jackson, M. R. Hurst, R. Leo, R. Lee, N. M. Landreville, A. K. Mishra, Y. Wang, and R. Sardinas, "NIST Cloud Computing Forensic Science Challenges," Tech. Rep. NISTIR 8006, National Institute of Standards and Technology, August 2020.

[27] M. Neovius, J. Karlsson, M. Westerlund, and G. Pulkkis, "Providing Tamper-Resistant Audit Trails for Cloud Forensics with Distributed Ledger based Solutions," *Cloud Computing*, vol. 2018, p. 29, 2018.

[28] H. Al-Khateeb, G. Epiphaniou, and H. Daly, *Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger*, pp. 149–168. Springer International Publishing, 2019.

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

[29] R. K. Naha, S. Garg, D. Georgakopoulos, P. P. Jayaraman, L. Gao, Y. Xiang, and R. Ranjan, "Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions," *IEEE access*, vol. 6, pp. 47980–48009, 2018.

[30] S. Singh, R. Sulthana, T. Shewale, V. Chamola, A. Benslimane, and B. Sikdar, "Machine-Learning-Assisted Security and Privacy Provisioning for Edge Computing: A Survey," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 236–260, 2022.

[31] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," Tech. Rep. Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, August 2020.

[32] R. Alkhadra, J. Abuzaid, M. AlShammari, and N. Mohammad, "Solar Winds Hack: In-Depth Analysis and Countermeasures," in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pp. 1–7, 2021.

[33] D. A. S. George, "When Trust Fails: Examining Systemic Risk in the Digital Economy from the 2024 CrowdStrike Outage," *Partners Universal Multidisciplinary Research Journal*, vol. 1, p. 134–152, Jul. 2024.

[34] J. T. Stoddard, M. A. Cutshaw, T. Williams, A. Friedman, and J. Murphy, "Software Bill of Materials (SBOM) Sharing Lifecycle Report," tech. rep., Idaho National Laboratory (INL), Idaho Falls, ID (United States), April 2023.

[35] Cybersecurity and Infrastructure Security Agency (CISA), "Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management." https://www.cisa.gov/resources-tools/resources/hardware-bill-materials-hbom-framework-supply-chain-risk-management, 2023.

[36] N. Sakimura, J. Bradley, M. Jones, B. De Medeiros, and C. Mortimore, "OpenID Connect Core 1.0," *The OpenID Foundation, specification*, vol. 335, 2014.

[37] A. Ometov, O. L. Molua, M. Komarov, and J. Nurmi, "A Survey of Security in Cloud, Edge, and Fog Computing," *Sensors*, vol. 22, no. 3, p. 927, 2022.

[38] D. Sabella, K. Maloor, N. Smith, M. Vanderveen, and A. Kourtis, "Edge Computing Cybersecurity Standards: Protecting Infrastructure and Applications," *IEEE Access*, 2024.

[39] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone, et al., "Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft)," *NIST special publication*, vol. 800, no. 162, pp. 1–54, 2013.

[40] C. Gentry, *A Fully Homomorphic Encryption Scheme*. Stanford university, 2009.

[41] D. Hardt, "The OAuth 2.0 Authorization Framework." RFC 6749, Oct. 2012.

[42] R. Bace and P. Mell, "Intrusion Detection Systems," 2001.

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

[43] A. Mac Dermott, Q. Shi, and K. Kifayat, "Collaborative Intrusion Detection in Federated Cloud Environments," *Journal of Computer Sciences and Applications*, vol. 3, pp. 10–20, July 2015.

[44] Trusted Computing Group, "Trusted Platform Module (TPM) 2.0 Library Specification, Part 1: Architecture." https://trustedcomputinggroup.org/wp-content/uploads/Trusted-Platform-Module-2.0-Library-Part-1-Version-184_pub.pdf, 2025.

[45] "Trusted Computing Group (TCG)." https://trustedcomputinggroup.org/.

[46] R. Perez, R. Sailer, L. van Doorn, et al., "vTPM: Virtualizing the Trusted Platform Module," in *Proc. 15th Conf. on USENIX Security Symposium*, pp. 305–320, 2006.

[47] A. Karakaya and A. Ulu, "A survey on post-quantum based approaches for edge computing security," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 16, no. 1, p. e1644, 2024.

[48] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Du˘sek, N. L¨utkenhaus, and M. Peev, "The Security of Practical Quantum Key Distribution," *Reviews of modern physics*, vol. 81, no. 3, pp. 1301–1350, 2009.

[49] "Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges," 2015. ETSI White Paper No. 8.

[50] D. Stebila and M. Mosca, "Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project," in *International Conference on Selected Areas in Cryptography*, pp. 14–37, Springer, 2016.

[51] D. Guha Roy, "BlockEdge: A Privacy-Aware Secured Edge Computing Framework Using Blockchain for Industry 4.0," *Sensors*, vol. 23, no. 5, 2023.

[52] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Hyperledger Fabric Blockchain for Securing the Edge Internet of Things," *Sensors*, vol. 21, no. 2, 2021.

[53] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukoli´c, S. W. Cocco, and J. Yellick, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *Proceedings of the Thirteenth EuroSys Conference,* EuroSys '18, (New York, NY, USA), Association for Computing Machinery, 2018.

This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)

Appendices

A.1 List of Acronyms

ABAC	Attribute-Based Access Control
API	Application Programming Interface
CRA	Cyber Resilience Act
DDoS	Distributed Denial of Service
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EU CSA	EU Cybersecurity Act
EUCS	EU Cybersecurity Certification Scheme
GDPR	General Data Protection Regulation
GSMA	Groupe Speciale Mobile Association
HBOM	Hardware Bill of Materials
IAM	Identity and Access Management
IAMS	Identity and Access Management Services
LEA	Law Enforcement Agency
MEC	Multi-access Edge Cloud
MISD	Modular Integrated Sustainable Datacenters
NIS2 Directive	Network and Information Systems Directive 2
OIDC	OpenID Connect
PFS	Perfect Forward Secrecy
QKD	Quantum Key Distribution
RED	Radio Equipment Directive
SBOM	Software Bill of Materials
SGX	Software Guard Extensions
SIEM	Security Information and Event Management
TCG	Trusted Computing Group
TEE	Trusted Execution Environment
TPM	Trusted Platform Module

MODULAR INTEGRATED SUSTAINABLE DATACENTER
Rijksdienst voor Ondernemend Nederland
8ra CLOUD-EDGE CONTINUUM
This activity is conducted in the scope of Modular Integrated Sustainable Datacenter (MISD) project which received funding from the Netherlands Enterprise Agency (RVO) under the 8ra initiative (IPCEI-CIS)