Bharat6G Alliance

Bharat 6G Alliance Whitepaper

6G Data Architecture, Security and Exposure Framework for RF Sensing

OCTOBER 2025

VERSION 1.0

Executive Summary

This white paper explores the 6G data architecture required to enable integrated sensing and communication (ISAC) capabilities, emphasizing the use of radio frequency (RF) sensing to unlock new applications across industries. It provides a detailed analysis of architectural, security, privacy, and data exposure challenges, while proposing a framework to address these issues. The document also highlights potential use cases, such as pollution monitoring, next-generation railways, and smart cities, and discusses the monetization opportunities and technical advancements necessary for successful implementation.

Key Findings

a. Integrated Sensing and Communication (ISAC): ISAC leverages RF signals for both communication and sensing, enabling applications such as autonomous driving, smart infrastructure, and environmental monitoring. Both monostatic and bi/multi-static sensing configurations are supported, with the latter requiring advanced synchronization mechanisms.
b. 6G Data Architecture: The architecture introduces SenseAct nodes for sensing and actuation, supporting both RF and non-RF sensors (e.g., LiDAR, cameras). Functional elements include sensing data exposure, processing, storage, and security, with APIs for discovery, requests, and access.
c. Privacy and Security: Privacy-enhancing technologies (e.g., differential privacy, encryption) are critical to protect sensitive data. Location-aware, object-aware, and user equipment (UE)-specific privacy profiles are proposed to ensure compliance with regulations such as the GDPR.
d. Monetization Potential: A "SenseGrid" concept, akin to a power grid, is proposed to incentivize data sharing and create economic value. Data marketplaces and frameworks such as Data Agreement Exchange-as-a-Service are identified as key enablers for revenue generation.

Risks

a. High Resource Demands: Sensing functionality requires significant compute, bandwidth, and energy resources, which may increase operational costs.
b. Privacy Violations: Improper handling of sensitive data could lead to regulatory non-compliance and reputational damage.
c. Security Vulnerabilities: Risks include data tampering, denial-of-service (DoS) attacks, and unauthorized access to sensing data.
d. Uncertainty in Sensed Data: Inaccurate or incomplete data could result in false alarms, undermining trust in the system.

Strategic Recommendations

a. Invest in Scalable and Configurable Architectures: Develop flexible sensing configurations to optimize resource usage and reduce costs.
b. Enhance Privacy and Security Measures: Implement robust privacy-enhancing technologies and ensure compliance with global regulations.
c. Foster Ecosystem Collaboration: Promote open APIs and data-sharing frameworks to enable third-party innovations and accelerate adoption.
d. Develop Monetization Models: Establish data marketplaces and incentivize stakeholders through transparent agreements and value-sharing mechanisms.
e. Prioritize Research and Development: Address challenges such as uncertainty in sensed data and synchronization in multi-static sensing to improve reliability and scalability.

This whitepaper underscores the need for a secure, scalable, and privacy-compliant 6G data architecture to realize the transformative potential of sensing use cases.

Table of Contents

1 Introduction

Radio Communication networks have blanketed almost the entire habitable portion of our planet. So far, these radio waves have been primarily used for telecommunication. From 6G onwards, they will also be used for sensing the physical world [1] leading to new applications in domains such as factory automation and security. Given the promise of integrated sensing, 3GPP study groups are exploring various aspects of its standardization. The 3GPP Technical Specification Group has released a feasibility study [2] on integrated sensing and communication, identifying several use cases, articulating service flows and outlining potential new requirements for supporting these capabilities in 6G networks.

This whitepaper captures the security and exposure challenges for the 6G data architecture required to enable sensing use cases. A reference 6G data architecture is proposed, considering these use cases. The aim of such a reference architecture is to address the following challenges inherent in integrated sensing and communication:

a. High computation and energy costs associated with the sensing functionality

   Sensing data from the radio network can consume substantial bandwidth, compute, storage, and energy resources. For example, a 200MHz bandwidth with 120KHz sub-carrier spacing leads to a data rate of 387.72 MB/s resulting in significant storage, compute, and energy costs. To mitigate these, the 6G data architecture should support configurable sensing functionality in terms of compute and bandwidth requirements. This will enable the operators to charge at finer granularity and allow application developers to optimize configurations by trading off accuracy with cost.

b. Privacy and Confidentiality related to sensing

   For publicly deployed networks, the sensing field may contain objects and regions belonging to one or more legal or personal entities. Private or confidential data might be captured; hence, the data architecture should provide mechanisms to filter sensed data based on entity consent. Such filtering should also be verifiable by independent means to ensure a high degree of trust. The architecture should support flexible and robust mechanisms for obtaining consent, setting access-control policies, and publishing relevant metadata about sensing capabilities.

c. Enable third-party innovations

   A microservice-based 6G data architecture, with open APIs and rich metadata about system components will foster a vibrant ecosystem of sensing services. An open-source reference implementation can further accelerate adoption and enable sustainable sensing services with reduced cost and increased flexibility.

d. Extreme Scalability

   The number of smartphone users is expected to reach about 6 billion by the end of this decade [3]. Correspondingly, radio controller nodes could scale to 60 - 150 million. This

will result in multiple interconnected management domains and the 6G data architecture must ensure interoperability cross them. Such capability will allow developers to build and deploy planet-scale sensing services seamlessly.

e. Support for the "SenseGrid"

Analogous to a power grid that enables energy generation and value attribution to end users, helping them to defray their utility costs, the 6G data architecture should facilitate value flow to the end nodes contributing sensing data, thereby creating a "SenseGrid." This will promote economic incentivization for distributed sensing and enable a new class of large-scale applications.

f. Incorporation of non-Radio network sensors

The 6G data architecture should also integrate non-radio sensors. Examples include hyperspectral imagers (for satellite-based base stations), cameras and LiDAR (for external radio units), built-in cameras, GPS and IMUs (for smart phones), and environmental sensors such as pollution, temperature, and humidity sensors (for fixed IoT devices). In connected vehicles, telemetry and on-board cameras add further modalities. Such multimodal data will enable rich applications and since privacy and compute challenges are common to all, the architecture should provide a unified framework to address them holistically.

Section 2 and 3 present a survey of the current standardization efforts in 3GPP, IEEE, and TSDSI including India-specific use cases. Section 4 discusses the associated challenges in detail. Sections 5 and 6 illustrate a potential 6G data architecture and its corresponding security profiles, while Section 7 identifies areas for further research.

2 Current Standardization Status

2.1 3GPP Release-19

3GPP SA WG1 has conducted study on various use cases and potential requirements for enhancements of the 5G system (5GS) to provide sensing services. The study was focused on use cases covering different verticals and applications, e.g. autonomous/assisted driving, V2X, UAVs, 3D map reconstruction, smart city, smart home, factories, healthcare, maritime sector. Figure 1 shows a comparative landscape of various use cases addressed by SA1 study and corresponding requirements identified.

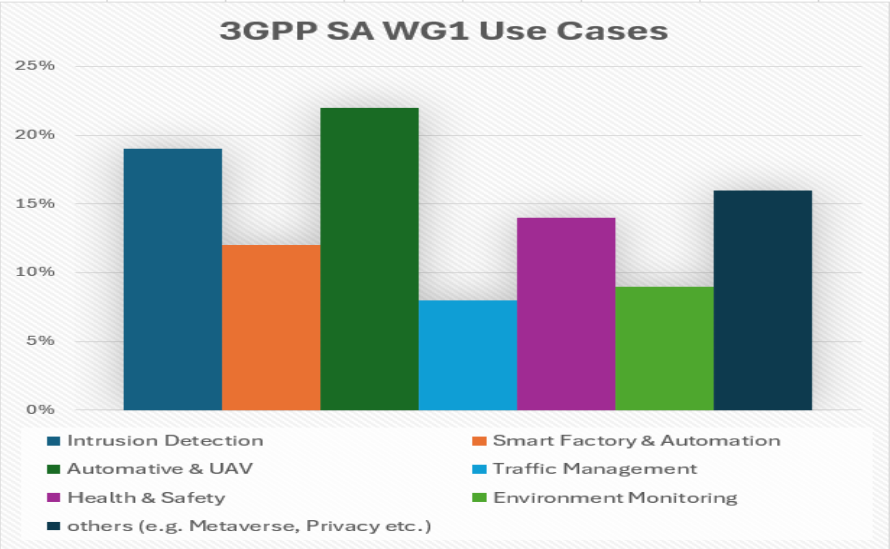


Figure 1: 3GPP use cases on Sensing

Although the primary focus of the study and corresponding requirements is to use 3GPP radio-based sensing, sensing data from authorized non-3GPP sensors (e.g. video, LiDAR, sonar etc.) could also be used in combination with the NR sensing data sensing data, to achieve improved sensing result or to enhance the sensing service. The corresponding stage-1 requirements, i.e., the functional and performance requirements for 5G wireless sensing service are specified in 3GPP TS 22.137 [7].

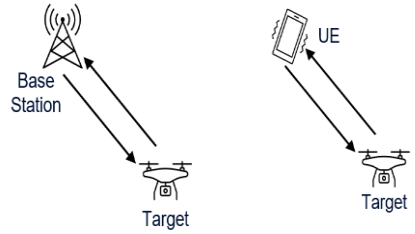


Figure 2: Monostatic sensing

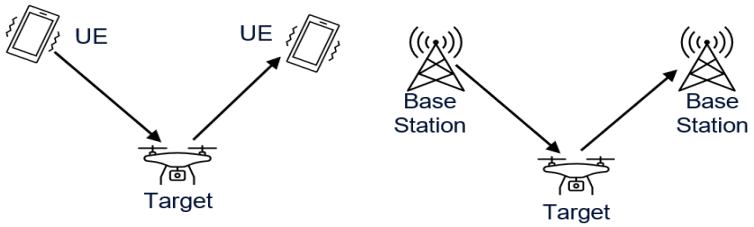


Figure 3: Multi-static sensing

It is possible to have both Monostatic and Bi/Multi-static sensing using 3GPP radio. The reception points are same, which could be either a Base Station or a UE.

In Monostatic sensing, the transmission and the reception points are same, which could be either a Base Station or a UE. That is, the transmission antenna that transmits a sensing signal and the receiver antenna that receives the echo of that transmitted sensing signal are collocated in the same Base Station or the same UE.

In Bi/Multi-static sensing, the receiving antenna is not collocated in the same entity as the entity transmitting the sensing signal, which also means that the transmitting and receiving antenna can be at different locations. The transmitter and receiver can be hosted in different Base Stations (Bi/Multi-static Base Station based), or they could be hosted in different UEs (Bi/Multi-static UE based) as shown in Figure 3.

There is also a possible configuration where a combination of Base Station and UE can be used for the sensing procedure where one Base Station can act as the transmitter and one or more UEs can act the receiver or vice versa (See Figure 4).

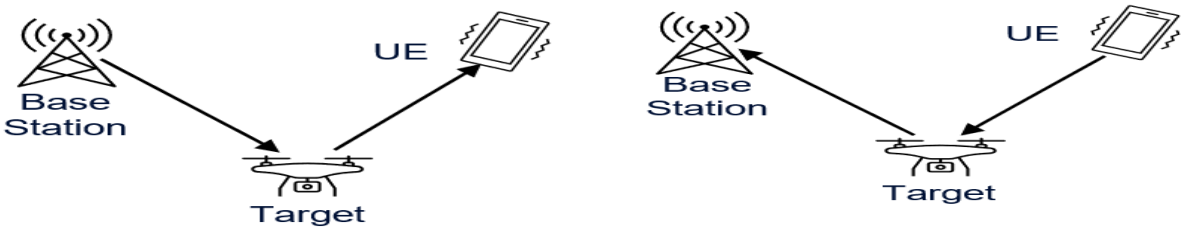


Figure 4: Multi-static UE assisted

In traditional radar applications (e.g. Airplane, Car, Ship etc.) Monostatic sensing is the most used technology and is also considered to be less complex to implement. The Bi/Multi-static sensing type will have comparatively complex design as it would need framework for synchronization between the transmitting and receiving entities to keep track on when to listen for an echoed transmitted sensing signal and also to coordinate the transmissions to reduce interference.
In 3GPP Release-19, based on the 3GPP SA WG1 identified service requirements, 3GPP RAN WG1 has started a study on Channel modelling to support 3GPP radio-based sensing. The 3GPP SA WG2 and 3GPP SA WG6 have also endorsed potential objectives to study the architectural enhancements and application enabler enhancements needed to support Integrated Sensing and Communication (ISAC).

2.2 IEEE 802.11BF WiFi Sensing

IEEE 802.11BF [4] defines the specification to identify the environment by Wi-Fi signaling apart from the communication. These mechanism covers the number of use cases such as:

- Gesture recognition.
- Remote health monitoring. Home security by motion detection.

WiFi sensing supports monostatic sensing, bistatic sensing and multistatic sensing [5]. WiFi sensing specifies PHY and MAC protocols and the corresponding application layer development is implementation specific.

2.3 TSDSI study on application level integrated and joint sensing

There is ongoing study in the TSDSI that explore the possibilities of different use cases of sensing. The report [6] talks about non 3GPP sensing and its related use case. Non 3GPP sensing (like Camera) devices are mounted on the already deployed base station (BS) infrastructure deployed across the country, by mounting the camera-based sensing on the BS infra. Thus, the operator can monetize sensing use cases in the existing network itself. Some of the use cases mentioned in the whitepaper are:

- Use case of intruder detection (Outdoor)
- Use case of intrusion detection (Indoor)
- Use case of Data Fusion for specific use case
- Use Case on Transparent Sensing Use Case
- Use case on sensing for Agritech
- Use case on sensing assistance for railways, e.g., obstacle detection on railway tracks
- Use Case on Sensing Assisted Automotive Maneuvering and Navigation

- Use case covering UAV flight trajectory tracing, etc.

3 Additional use cases

3.1 General

As captured in Section 2, different standardization bodies are exploring different use cases. This section captures additional use cases which are foreseen.

3.2 Pollution sensing

3.2.1 Introduction

Ambient air pollution monitoring and adoption of various techniques to mitigate hazardous impact of the increasing pollution on human health is a global concern. From the Indian perspective, rapid growth of the economy and urban infrastructure including deforestation has resulted into a significant hike in the air pollution levels in the past few decades. Considering, large scale commercial roll-out of 5G networks pan-India and Government's Bharat 6G Vision, the concept of Integrated sensing and communication (ISAC) can be leveraged which is one of the enablers for 6G. ISAC can be used both in active and passive framework for ambient pollution monitoring.

3.2.2 Passive

In this mode the ISAC framework can be coupled with conventional physical air pollution sensor measurements to come up with a holistic ambient air pollution sensing framework. Depending on the diffusion pattern over the air and the measured concentration of various pollutants that includes gases like ammonia (NH_3), hydrogen sulphide (H_2S), carbon oxides (CO_x), nitrogen oxides (NO_x), sulphur oxides (SO_x),methane (CH_4), suspended particulate matters (SPM) at precise geographical locations, it is possible to come up with efficient mathematical model to predict the pollution concentration levels for mapping the pollution hotspots for areas where dense physical sensors deployment is not feasible as for example highways. In this case the mathematical model can leverage on the ISAC framework. The reflected radio waves from vehicles or areas with dense human activities which actively contribute towards significant ambient pollution can be sensed by the nearest based station. The base station can now estimate the distribution of the average traffic flow or duration of localized human activities at given areas (for e.g. office area or tech parks etc.). This spatial-temporal distribution of the traffic load or human activities obtained using ISAC framework can be integrated with the existing state-of-the art mathematical models.

3.2.3 Active

Fine granular quantification of the air pollution levels that includes the concentration of the ambient air gas elements such as ammonia (NH_3), hydrogen sulphide (H_2S), carbon oxides (CO_x), nitrogen oxides (NO_x), sulphur oxides (SO_x),methane (CH_4), requires calibrated sensors. Using reflected waves to quantify the accurate concentration of the gas or suspended particulate matter (SPM) can be a major technological challenge which requires further research. However, the EM waves operating in the Terahertz regime (0.3 -30 THz) are characterized by their absorption and attenuation caused due to the molecular absorption of various gases and water vapor present in the atmosphere. There are established models proposed by ITU and 3GPP which capture the impact

of such molecular absorption losses. Prior art is available where techniques such as a high efficiency, low-cost pollution air monitoring system based on space-borne terahertz radiometer monitoring SO3 and NH3 were proposed [9].
Similarly, new updated air pollution mitigation using pulse radio waves is an emerging technology for air pollution mitigation whereby the ambient SPM are charged using pulsed radio waves. Once charged the SPM eventually gets heavier and settles down. Sensing framework of the ISAC can be effectively used to detect the dissipated charge to quantify the SPM concentration [10].

3.3 Sensing for next-gen railways

International Union for Railways (UIC) has specified protocols for Future Railways Mobile Communication Systems (FRMCS) which can support data rate in the order of Gbps for a plethora of applications that includes European Train Control System (ETCS)L2/L3 signaling for rail-integrity and railways signaling (both on-board and trackside). Based on the inputs received from the UIC, 3GPP has already prepared the initial framework for the Stage-1 enhancements required to support FRMCS as described in [11].
A use case enabling FRMCS to setup data communication between infrastructure systems and a ground based or train based system in order to monitor or control critical infrastructure such as train detection, signals and indicators, movable infrastructure, level crossing elements, including barrier controls vehicle sensors, lighting controls and alarms, has been agreed as per proposed enhancement of FRMCS (3GPP TR 22.989). The stage 1 specification (3GPP TS 22.282) covered the mission critical parameters KPIs as for e.g. operator defined QoS and priority and setup time.
The basic architecture for FRMCS coupled with Integrated sensing and communication (ISAC) framework can have potential use cases that include unauthorized intrusion detection at the railway level crossings and the main railway track, early track fault detection warning, ETCS L2/L3 signaling enhancements including anti-collision mechanisms etc. In case of a generalized FRMCS architecture, the on-board applications and trackside applications use the 5G RAN and the core network to transmit data periodically to a remote centralized mission critical server. The mobile gateway on-board the railway is connected to the mission critical server over 5G NR based RAN and core architecture. The On-board and the trackside application clients along with their corresponding gateways and the cellular connectivity interface can be integrated with the ISAC framework. Some research in this direction was proposed in [12] where ISAC framework was coupled with high-speed railways (HSR) based mmWave network where two mmWave beams are intelligently controlled to provide broadband communications and environment sensing.
Furthermore, deep reinforcement learning (DRL) techniques was implemented to mitigate the adverse impacts of inter-beam interference between the communicating and the sensing beams. In [13], a ISAC framework assisted solution is proposed for virtual coupling which is part of ETCS L2/L3 signaling whereby solid-state LiDAR based sensing system was used to provide an accurate, robust and low-latency on-board distance detection system between trains.

3.4 3GPP 6G use cases

In 3GPP Release-20 3GPP SA WG1 is studying more use cases and service requirements for Integrated Sensing and Communication (ISAC) [17]. The use cases include ISAC applied to safety scenarios, drone monitoring, environment object reconstruction (Digital Twin) and monitoring, passive infrastructure digitalization (e.g. roads), smart transportation scenarios (e.g. detection of ships, vehicle state prediction), immersive reality, collaborative robots using Digital Twins, and many more.

4 Analysis of Security and Exposure for 6G Data Architecture

4.1 Security/Privacy aspects

Technical Specification document 3GPP TS 22.137 [7] covers the service requirements for Integrated Sensing and Communication (Stage 1, Release 19). This section provides an analysis of security and privacy aspects challenges that are associated with telecom level sensing.

a. Security issues
   - Integrity of data: Sensing signal and sensing data will contain objects and regions information corresponding to one or more legal or personal entities and operator has to store these data for different sensing use cases. The alternation of this sensing data may lead to tampering issue. Attackers might alter the data being transmitted, leading to incorrect sensing information.
   - Denial of Service (DoS): Attackers can flood the base station with traffic, causing legitimate sensing and communication functions to be disrupted.

b. Privacy issues (Location related privacy):

   GDPR (General Data Protection Regulation) states that all forms of surveillance must abide by specific rules. The most important of them is the right of EU residents to information about the kind of data that is extracted (voice, gesture, video, etc.), its quality (resolution of recording or data collection), and its use (is it shared with a third party, stored or processed on the spot). Telecom sensing is also considered as a form of surveillance and all GDPR rules and regulations will also be applicable to telecom sensing. As sensing is strongly believed to be a part of a telecom network, the technical question is here: how to inform the UEs (e.g., vehicles, smart phones) that are in the sensing zone about the collection of their sensed information. Furthermore, the quality, duration, and periodicity of the sensing process need to be publicly shared via certain types of messaging. This is a crucial responsibility of the sensing party. The existing privacy mechanisms defined for location services defined in 3GPP TS 23.273 [8], have been developed with, as a core part of their rationale, a specific UE, described, e.g., by its Subscription Permanent Identifier (SUPI). However, this is not adequate for the sensing services. This is because the existing privacy profile data does not support many of the privacy requirements that several use cases have, such as:
   - to allow or not the sensing of a defined region or geographical area (non-UE privacy aspect)
   - to allow or not the detection of connected objects that do not have a SUPI or in general cannot be described with communication related identifiers.
   - to obfuscate or hide or change important/sensitive features (e.g., size, shape, etc.,) of detected objects.

The sensing requests from UE or telecom network should also pass through the required privacy

checks, since the area around UE may include sensitive data (e.g., objects, features, etc.,). Continuous data collection can lead to detailed profiles of individuals' behaviors and preferences, which may be exploited. Secondly, Data collected for one purpose may be used for another without user consent, leading to privacy violations.

4.2 Exposure related challenges

As part of the sensing use case, the sensing data or data representing sensing object has to be exposed to the external consumer such as application function (AF), i.e. outside the telecom network. The following challenges are envisioned for further study:

a. Sensing data/object model: The data representation of the sensing data/object can be based on a generic sensing data/object model or be based on certain classifications. The sensing data/object model also provides a perspective on the abstraction levels, volume/size of data involved for the exposure.

b. Sensing data exposure methods: Depending on the use case the following exposure methods can be envisioned:
   - Sensing data streaming exposure: The AF may consume stream of sensing data in real-time depending on the use case. It may have different streaming data rates coupled with different volume/size of sensing data.
   - Event-based exposure: The sensing data exposure can be designed as events, which can be subscribed by the AF depending on the use case.
   - On-demand exposure: The sensing data exposure can be modeled using a query-response method. Depending on the use case, the AF may request certain sensing data information and the network provides the requested data. It is required to discover the sensing data from a massive combination of real-time and historic data set within a defined SLA.
   - Filtered exposure: Context-aware filtering would also have to be considered [15]. This would ensure that only the data needed by the data consumer would be made available.

5 Reference 6G Data Architecture

5.1 Architecture

A reference 6G data architecture is illustrated in Figure 5.

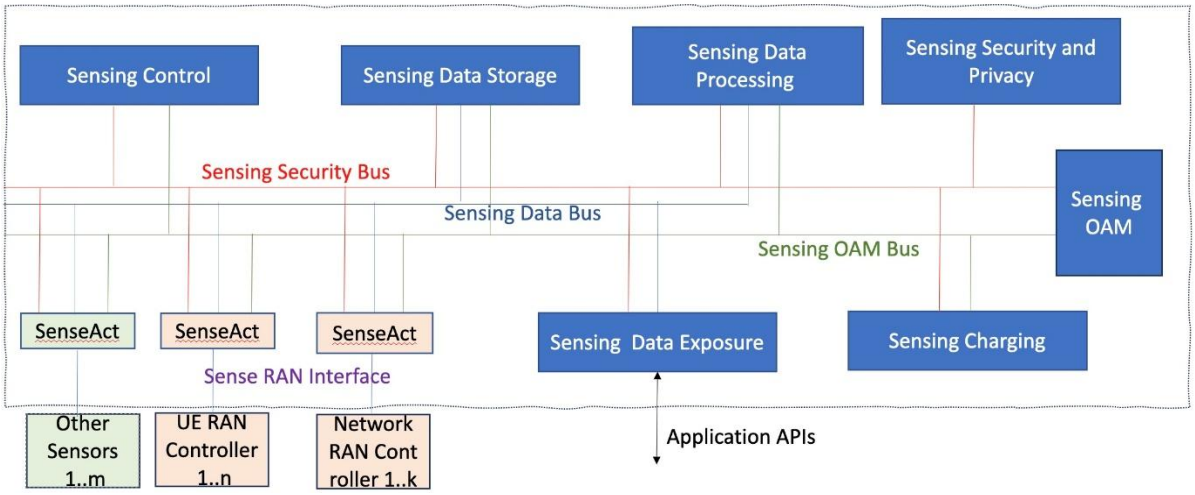


Figure 5: Reference 6G Data Architecture (for Sensing)

NOTE: The SenseAct nodes are attached with the RAN and connected to the radio controllers.

5.2 Functional Elements

5.2.1 Sensing Data Exposure

5.2.1.1 Overview

This element provides the exposure interface to end applications that need the sensing data. It exposes service APIs for applications to discover, request and consume sensing data. The APIs can be categorized into the following groups:

a. Discovery: Discover the sensing services available including the data formats/ontologies, their associated costs and billing information and security & privacy requirements
b. Requests: Register requests for using sensing services, including security credentials, as well as request specific sensing functions
c. Access: Access sensing data and associated telemetry

Further, the functional element interacts with all the other functional elements of the system to support the realization of the exposure APIs. This section provides detailed description for each group of APIs.

5.2.1.2 Discovery API group

Self-reporting of available sensing services and their requirements, in a standardized format, will allow for scalable, vendor neutral and future proof solutions to evolve. The key requirement will be to standardize the data models/ontologies to capture all the relevant information needed for consumer application developers.

An example data model for exposing sensing service is:

Name	Data Type	Description
Sensing Service Name	String	Semantic identifier for this service
Sensing Data Description	String	Explanation about the sensed data, its limitations, applicability etc.
Sensing Data Model	URI	Link to JSON/XML template describing the data model for the sensed data in more detail.
Sensing Parameter Model	URI	Link to JSON/XML template describing the data model for the service's parameters. This could include items like frequency range choices, modulation format choices, beam directions, etc.
Sensing CPU Load	Integer	CPU Ops needed per sensing operation
Sensing GPU Load	Integer	GPU Ops needed per sensing operation
Sensing Rate Min	Integer	Minimum rate for sensing
Sensing Rate Max	Integer	Maximum rate for sensing. Rate of 0 will indicate one time sensing
Sensing Latency Min	Integer	Minimum Delay between physical initiation of sensing, to exposure via API
Sensing Latency Max	Integer	Maximum delay between physical initiation of sensing, to exposure via API

Table 1: Data model for exposing sensing service

A catalogue service can be run separately – that could provide a searchable interface for all available services and their pricing.

5.2.1.3 Requests API group

Applications that want to consume sensing data, will request specific sensing services using these APIs. A key component of this interface will be related to security and privacy checks. This will have workflows to authenticate the requester, authorize access to the specific sensing resources and validate & set the privacy levels for the sensing data. These tasks will be performed with the help of the Sensing Security & Control element, over the Sensing Security Bus. As there will be a separate sensing data stream/Bus, their security requirement will also be different. Once the requester is authenticated and authorized, admission control decision will be taken by the Sensing Configuration & Provisioning element based on available sensing resources and the requester's priority. It will lead to either granting, denial or deferment of the request. Once a request is granted, appropriate security tokens as well as a unique sensing session identifier will be issued, which will be needed to access the sensing data. These tokens will embed the security & privacy authorization and authentication information, as well as encryption keys.

5.2.1.4 Access API group

Sensing data will be exposed via these APIs to end applications. Data access will be guarded by security mechanisms. The APIs will support both REST style as well as streaming interfaces. Separate APIs will also allow extraction of telemetry data – relevant to sensing functions. These can be used by the application to validate SLAs, KPIs etc.

5.2.2 Sensing OAM (Configuration & Provisioning)

This functional element does the scheduling and provisioning of sensing resources for authenticated and authorized sensing requests. It uses real-time information about the availability of sensing resources across the UEs, Radio Units, as well as compute resources in the Sensing Data Processing element and allocates

these resources for satisfying the sensing requests. Prior to provisioning, the access control, security and privacy check will be carried out by analyzing the access control and privacy settings against the certificates of the functions in the sensing processing chain.

5.2.3 SenseAct Nodes in UEs and Base Stations

5.2.3.1 Overview

A SenseAct node provides Sensing functionality, and its core elements are shown in Figure 6.

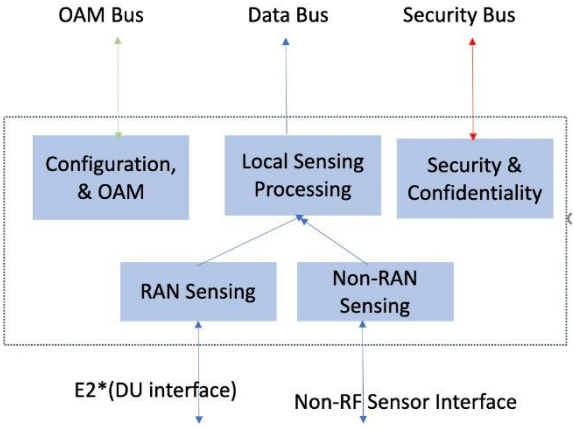


Figure 6: Key constituents of the SenseAct functional element

This functional element can gather either RF based sensory data (from the Radio Units) or non-RF sensory data from other sensing elements.

For passive sensing, the information and energy flow are unidirectional – from the transducer into the sensing logic. For active sensing, a stimulus to the physical system is usually needed to achieve the sensing functionality. Such a stimulus is referred to as Actuation. For example, in the case of mono-static radar, the standard communication signals suffice to extract the information of the channel and hence the range and speeds of objects therein. However, for bi-static or multi-static radar, one station will need to actuate by actively transmitting specially coded signals, and the other stations will receive the resultant signals and complete the sensing function.

Hence, active radio-based sensing will involve transmitting beacons or RF pulses/signals with specific modulation, power, direction and duration and will be configurable as part of the actuation functionality of the SenseAct element. It is assumed that each SenseAct node has access to a global timing reference signal. The accuracy of certain sensing services will depend on the timing accuracy of this synchronization signal. The architecture allows for a synchronized actuation from more than one SenseAct node. The node implementing the sensing function might be different from the node implementing the actuation function as in the case of multi-static radar.

The architecture allows for a uniform way to ingest non-RAN based sensors – example video or lidar images, pollution sensors etc., which might be attached to the UEs or Radio Units. This enables such sensing data to be governed by the same architecture – and will get the benefits of privacy, access control, multi-modality etc.

When a SenseAct function will need to use the radio resources at the UE or the Radio Unit, it will have a standard interface F1 to the L2 layer of the Radio Units in UE and Base Stations. This will be a high bandwidth, synchronous interface, time synced to TTI interval of the DU.

When the SenseAct function needs to use non-RAN based resources, it will have appropriate interworking APIs to access those. However, the interfaces on the Sensing OAM, Data and

Security buses will remain same, thus providing a uniform method to access RAN and non-RAN based sensing resources.
The SenseAct nodes will expose the available sensing resources (for actuation, sensing and local compute) to the Sensing Configuration & Provisioning element upon initial attachment as well as periodically over the Sensing OAM bus.

5.2.3.2 SenseAct Functions and Possible Architecture Impacts

Figure 7 illustrates a reference architecture to support the SenseAct function in a split view 6G RAN node. The impacted RAN entities and interfaces are highlighted.

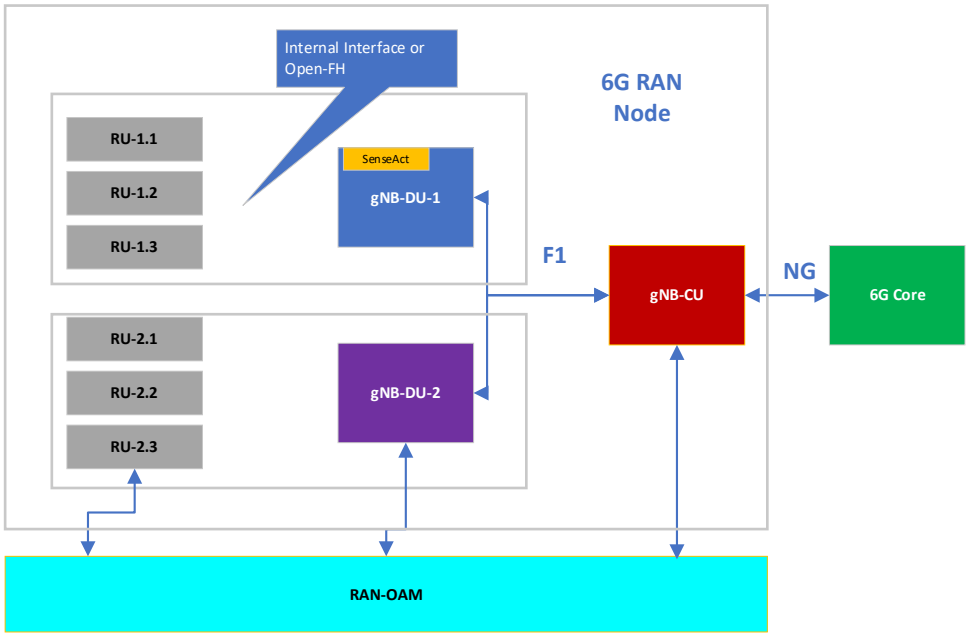


Figure 7: 6G RAN node reference architecture to support SenseAct function

In the above architecture, the SenseAct logical function is assumed to be part of the gNB-DU of the RAN node. It is to be noted that the function could be part of a few or all of the gNB-DUs.

a. Impacted Interfaces for SenseAct Function
   - OpenFH or proprietary interface between the RU and DU
   - F1 between DU and CU (both F1-C and F1-U)
   - NG interface between the RAN and Core (both NG-C and NG-U)
   - Interface between the RAN-OAM and RAN functional entities like DU/CU/RU

b. Functionality Support

The configuration of the SenseAct function could be done in various ways.

- RAN-OAM could locally configure the various aspects – radio resources for example.
- There could be partial configuration coming from the 6G core, particularly for those parts that are common across 6G RAN nodes.

c. Sensing measurements

- The RUs are configured to transmit and measure the UL sensing data of interest in the form of I/Q samples.
- Measurements are then sent in the UL from RU to DU to CU.
- The final consumption of the measurements is in the 6G core.

d. Radio Resource Management
   - The radio resources for sensing should co-exist with that for normal RAN operations – signaling, user data etc., This is to be managed at the DU/CU level across the SenseAct nodes.

5.2.4 Sensing Data Processing

Sensed data will undergo one or more levels of processing. The functions applied to this processing will be sourced from the sensing data hub. The processing functions' signature, authorization and ownership will be validated prior to running them. The sensor data processing will use a streaming paradigm where data flows continuously in one direction from the sensors. Sensing functions will be packaged in an appropriate runtime with light weight containerization – to ensure decoupling from the physical architecture of the underlying nodes. Compute orchestration will be handled by the Sensing Configuration & Processing element. Communication between the processing functions, exposure element and storage will be over the sensing data bus. Processing paradigms could be event based or streaming based and is left flexible for future implementation choices.

5.2.5 Sensing Charging

Sensing charging maintains the costs for usage of the sensing services at different granularities of resource consumption as well as time (charge per month, versus charge per sensing transaction, object based). It can implement various billing and charging functionalities – as are legally allowed within the governance domain of the sensing infrastructure. Sensing Data Hub. This element hosts various repositories related to the sensing services.
Certified sensing functions will be hosted in a repository, to enable deployment of these as and when needed. Log information from all the elements, and their transactions will also be hosted in this hub. This information will be used for auditing functionalities for the service provider. Storage of a limited amount of sensing data may also be provided as a service to end consumers. This storage service will be configurable in terms of what subset of data to store and what is the maximum quantity.

5.2.6 Sensing Data Storage

This element is responsible for storing raw sensing data and the processed sensing data. Such stored data can be used for statistical analysis and AIML model training.

5.2.7 Sensing Control

This element is responsible for setting the detailed profile configuration of the SenseAct elements based on Sensing OAM information.

5.3 Sensing Communication Bus

5.3.1 Sensing OAM Bus

The internal communication for Operations, Administration and Management, will be over this bus. Since the OAM functionality encompasses all the elements, every element will be on this bus. Examples include live telemetry information, internal resource discovery messages etc.
The bus can support multiple communication paradigms like request-response, publish-subscribe etc. The underlying communication network will be an IP network. This includes connection with the UEs and the Base station radio units. All communications will be protected via TLS (Transport Layer Security) mechanism and will need strong authentication to access the bus.
This bus can be implemented using any of the many available technologies for IP based messaging network. The bus is never exposed to the external sensing data consumers and is only available for the Sensing service provider – thus enhancing the security of the system.

5.3.2 Sensing Data Bus

The sensed data traffic be of high bandwidth and will also be latency sensitive. In addition, the data will be of a sensitive nature – and hence will need good security features. The data communication will be unidirectional – flowing from SenseAct nodes towards the Sensing Processing Element and finally towards Sensing Exposure element. The data stream will be protected via appropriate security protocols.
Sensing data will be made available from the designated sensing processing element, only via the sensing exposure element via the access APIs. This access will also be provided only to authenticated and authorized entities, thus maintaining security and privacy. The unidirectional flow of data is sufficient to handle desired functionality of sensing data processing and exposure. It also enhances the security of the system as the recipient of the intermediary data is not broadcast to an unlimited set of downstream nodes. At most, there can be a fork to save the data in the storage hub.

5.3.3 Sensing Security Bus

To minimize the security vulnerabilities of the overall system, all security related communications will be supported by a separate bus, independent of the data and OAM buses.
The security bus will be protected by its own TLS methods and will be IP based. All security related messaging like provisioning of certificates, authentication, authorization, privacy policy updates, etc., will happen over this bus.

5.4 Simplified Call Flow

Figure 8 provides an illustration of a simplified call flow depicting interactions involving a consumer (e.g. Application Function – AF), producer (e.g. Sensing Data Exposure) and various functional elements of the 6G Data Architecture.

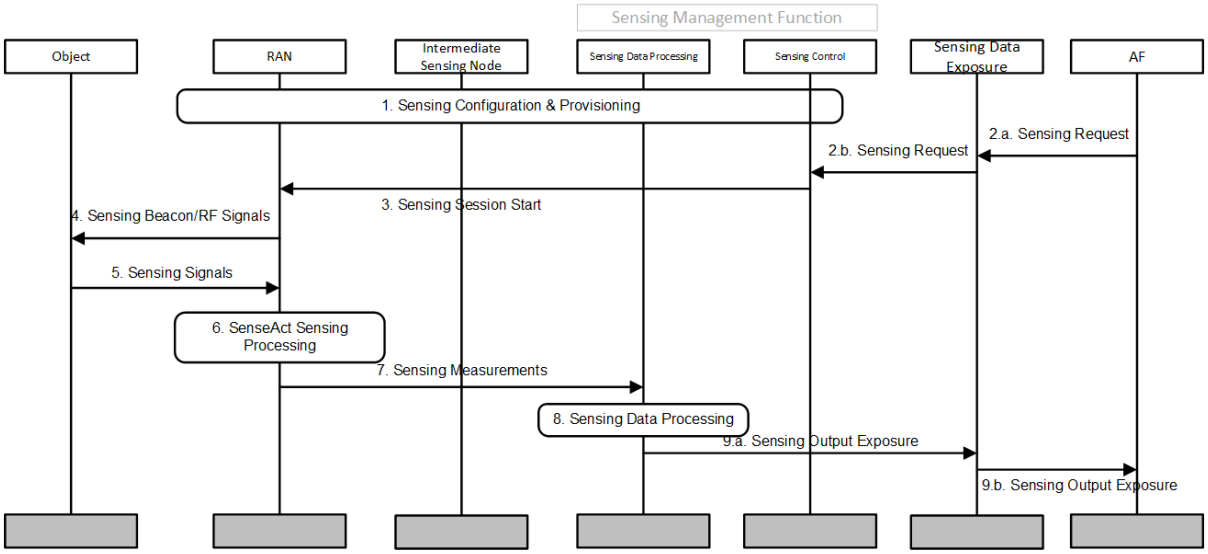


Figure 8: Simplified call flow depicting sensing functionality

6 Security profiles for 6G Data Architecture

To solve the privacy and security issues related to sensing, new privacy profiles should be defined and stored in the telecom (Core) Network to allow or disallow the sensing service. Telecom network must respect the privacy profile before or during the sensing operation. Three types of privacy profiles have been identified:

a. Location-aware Sensing Privacy: The Location-aware Sensing Privacy indicates whether allows or disallows the subsequent sensing requests in a specific area. It may include Geographical area description, e.g., using GPS coordinates, everywhere, etc. to allow to disallow the sensing.

b. UE Sensing Privacy Indication: The UE Sensing Privacy Indication indicates whether allows or disallows the subsequent sensing requests for a specific UE and/or whether to be involved in the sensing procedure. It may include user preferences. It also contains the policy to enable obfuscation of features of the object.

c. Object-aware Sensing Privacy Indication: And the Object-aware Sensing Privacy Indication indicates whether allows or disallows the subsequent sensing requests for a specific object, according to the respective descriptors. It may include one or more object type and details of details of the object. Example, certain government building should be obfuscated from the sensing output.

Privacy/Confidentiality of the sensing data will be determined according to the following classes:

Level	**Description**
Raw	Raw sensing data, as is, will be exposed
privacy enhanced method	Sensing private data will be processed with privacy enhanced method,

	example, Examples: Differential Privacy, Information theoretic privacy, K-anonymization etc. Various anonymization functions will be made available as part of the sensing data processing.
Pooling	Access to a set of available functions of the sensing data will be available. For instance, some statistics, e.g. Expected Value, Variance, or Max/Min.
Encrypted	Sensing data will be encrypted using one-way encryption functions (e.g. holomorphic)

Table 2: Privacy/Confidentiality classes

The network will also facilitate audits of all processes and transactions both within the system as well as with external entities, by using the logs maintained in each element. Secondly to inform the user that the user is being monitored by telecom sensing service, the telecom operator should expose the information of sensing via different means. i.e. broadcasting via SIB (radio signals), sending SMSs, providing information via portal etc. This information may also contain the geographical area that is being sensed. If operator is required to expose the sensing data, it is required to enhance the exposed private data by an appropriate privacy enhancing technology.

7 Areas for further research

7.1 General

The distortions and impairments in the modulated RF waves used for communication become "signal" for sensing applications. However significant computation is required to extract meaningful information from these. On the other hand, specially crafted RF signals just for sensing purposes will incur significant additional hardware costs and might not be suitable for widespread deployment. Hence the sensing framework in 6G will need to support a judicious and configurable partitioning of compute and radio resources between these two functionalities. Given the high bandwidth and processing requirements of RAN sensing data, raw data will seldom be transmitted as is, but instead various algorithms will need to be run locally to extract and send only meaningful information. Since 5G, the RAN functions are fully implementable in software on high performance local compute. Hence RF sensing processing. becomes another software module and can largely time share the compute infrastructure that is already created for handing communication.

Sensing carries with it the twin challenge of security and privacy. Hence the sensing framework is required that should support the enforcement of privacy policies, while ensuring the application of all relevant security policies. It is specially required in case of sensing data exposure. Sensed data can be a valuable economic asset; hence the framework allows for distributed value creation and support for various credit attribution policies. Along with strong privacy mechanisms, the sensing framework will then allow for enabling new dimensions to the economy, like the emergence of the SenseGrid – much like the power grid. This can be operationalized via an approach such as DAES presented above in Section 7.2. Such a framework, enforced by the telecom network, will also provide the necessary infrastructure to handle even non-RAN based sensing data. Further research is required for data streaming protocol(s) within 6G network, exposure defined for wider application community usage. The specification of privacy policy and its realization has to be explored.

7.2 Monetization aspects

Considering the central importance of data in 6G, two questions arise: (1) how can data providers be incentivized so that they are willing to share data which can be picked up by sensors, and (2) how can this data then be utilized by network operators to generate revenue from their clients? This necessitates the idea of a "data marketplace" that incentivizes all stakeholders in the data generation and consumption process to participate and achieve mutual benefit. This would require the specification of data contracts [16] between the data generators and network operators, and between network operators and their clients. These contracts should clearly specify what data the consumer would be allowed to access, in what granularity, what use the consumer would make of the collected data, and to whom the consumer is allowed to share the data in order to ensure security and privacy. In [16], a Data Agreement Exchange as a Service (DAES) is presented, which is illustrated in Figure 9.

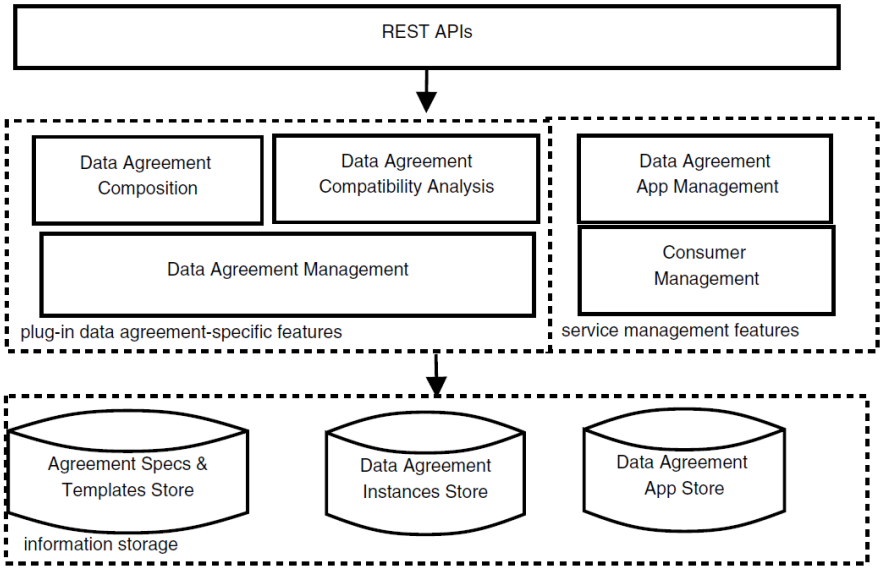


Figure 9: Overview of Data Agreement Exchange as a Service (DAES) [16]

DAES aims at being a cloud service for data marketplaces in which different data agreement specifications can be registered, multiple Data as a Service (DaaS) providers, data providers and data consumers can use DAES to exchange their data agreements, and several agreement-specific operations, such as creation and validation, composition, and compatibility analysis, can be supported.

Some possible data interaction models for data enriched as part of agreements, is presented in Figure 10.

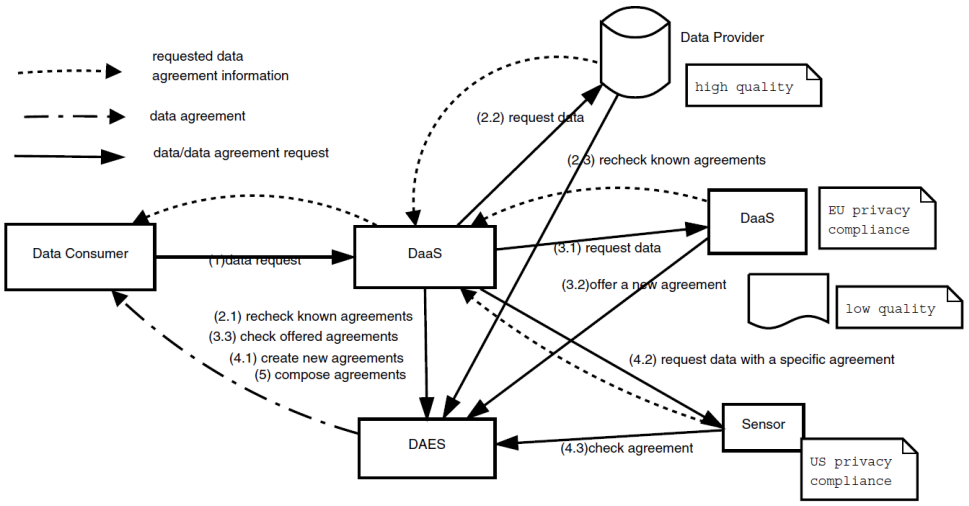


Figure 10: Possible interaction models for data enriched with data agreements [16]

Referring to the 6G Data Architecture illustrated in Section 5.1, how to integrate a monetization model like DAES is for further study.

7.3 Uncertainty in Sensed Data

Early warning in the presence of uncertainty in sensed data will create enormous false alarms and few genuine alarms. The application scenario may include safety communications in FRMCS, intrusion detection in supply chain management [19, 20], and condition monitoring in factory floor. Root cause analysis (RCA) with causal data and their relationship will provide high confidence in the alert generated in these use case scenarios [14].
How to prevent uncertainty in Sensed Data is for further study.

8 Acknowledgement

This research was conducted by Indian Institute of Science/ARTPARK and supported by Nokia.
Many thanks to the co-authors from Indian Institute of Science (IISc) Bengaluru, Nokia Solutions and Networks India Pvt. Ltd., Bharti Airtel, Vodafone Idea Limited, Indian Institute of Technology – Bombay (IIT-Bombay), Centre for Development of Telematics (C-DOT), HFCL, Tata Consultancy Services (TCS) for their valuable contributions and feedback.

9 References

[1]. 6G Integrated Sensing and Communication: From Vision to Realization, Wild et. Al., Joint Communication and Sensing in 6G, 2023

[2]. 3GPP TR 22.837 v19.2.1, Feasibility study on Integrated Sensing and Communication, Feb 2024.

[3]. https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

[4]. IEEE SA - IEEE 802.11bf Aims to Enable a New Application of WLAN Technology: WLAN Sensing

[5]. Wi-Fi Sensing Based on IEEE 802.11bf, IEEE Communications Magazine, Jan 2023.

[6]. WI-NIP310– Integrated communication and sensing at the Application level.

[7]. 3GPP TS 22.137: "Service requirements for Integrated Sensing and Communication; Stage 1".

[8]. 3GPP TS 23.273: "5G System (5GS) Location Services (LCS)".

[9]. R. You, Z. Lu, Q. Hou and T. Jiang, "Study of pollution air monitoring system based on space-borne terahertz radiometer," 2017 10th UK-Europe-China Workshop on Millimetre Waves and Terahertz Technologies (UCMMT), Liverpool, UK, 2017, pp. 1-4

[10]. R. Kantikar, R. C. Balan, K. Shinde and S. Sola, "Mitigation of Air Pollution Using Pulsed Radio Waves Technology in the Ambient Environment," 2022 International Conference on Environmental Science and Green Energy (ICESGE), Shenyang, China, 2022,

[11]. 3GPP TS 22.289: 3GPP Technical Specification Group Services and System Aspects; Mobile Communication System for Railways; Stage 1 (Rel-18).

[12]. L. Yan, X. Fang, S. Li, Y. Li and Q. Xue, "DRL Based Beam Management for Joint Sensing and Communications in HSR mmWave Wireless Networks," in proc. IEEE Vehicular Technology Conference: (VTC2022-Spring), Helsinki, Finland, 2022, pp. 1-6.

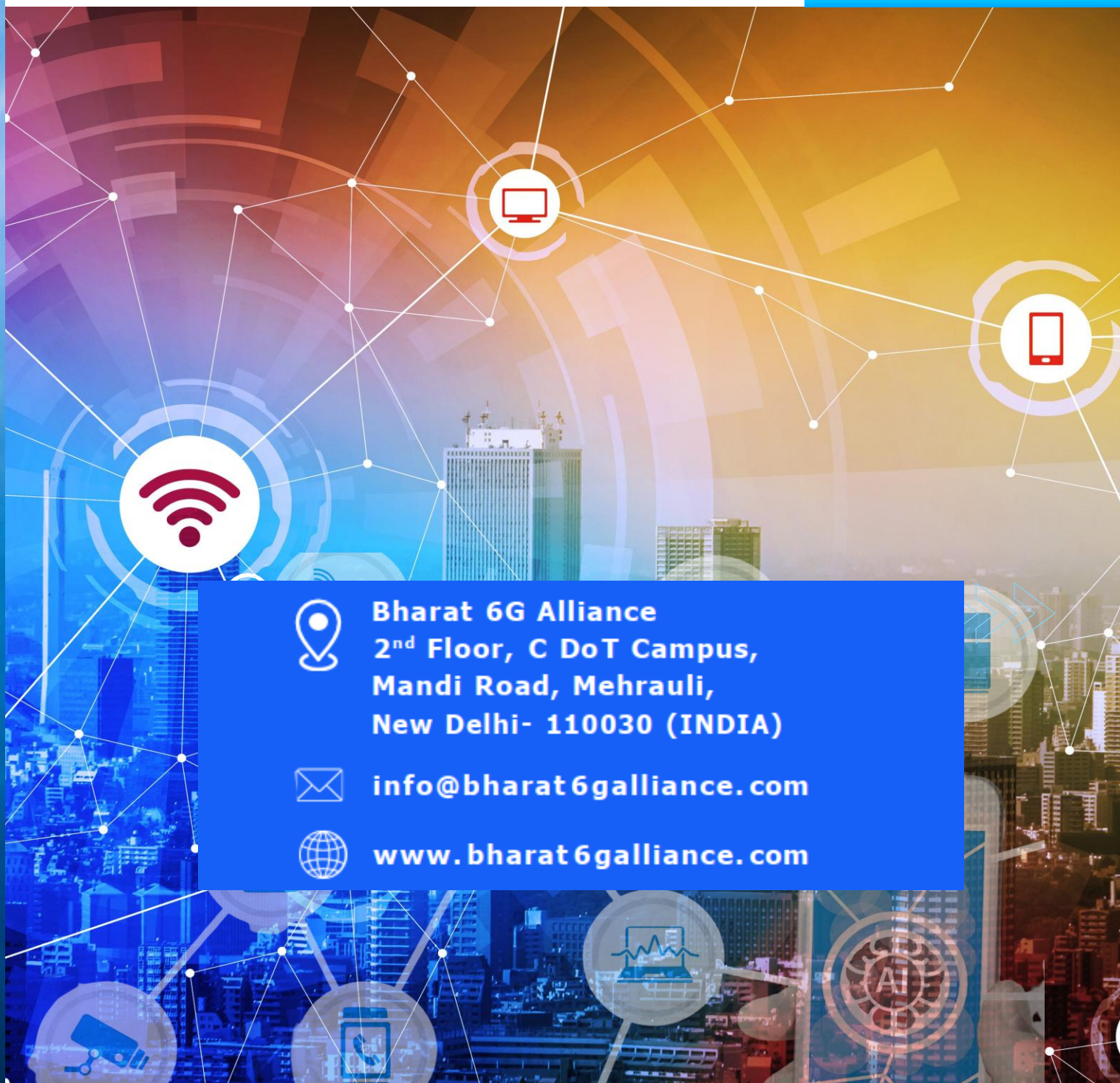
[13]. G. Mujica, J. Henche and J. Portilla, "Internet of Things in the Railway Domain: Edge Sensing System Based on Solid-State LIDAR and Fuzzy Clustering for Virtual Coupling," in IEEE Access, vol. 9, pp. 68093-68107, 2021.

[14]. Vijay, Rathinamala, and T. V. Prabhakar. "Causal AI for cable health monitoring." Measurement (2025): 117705.

[15]. Narendra, N., Ponnalagu, K., Ghose, A., & Tamilselvam, S. (2015, September). Goal-driven context-aware data filtering in IoT-based systems. In 2015 IEEE 18th International Conference on Intelligent Transportation Systems (pp. 2172-2179). IEEE.

[16]. Truong, H. L., Dustdar, S., Gotze, J., Fleuren, T., Muller, P., Tbahriti, S. E., ... & Ghedira, C. (2011, December). Exchanging data agreements in the daas model. In 2011 IEEE Asia-Pacific Services Computing Conference (pp. 153-160). IEEE.

[17]. 3GPP TR 22.870 v0.3.1, Study on 6G Use Cases and Service Requirements, Jun 2025.



Bharat 6G Alliance
2nd Floor, C DoT Campus,
Mandi Road, Mehrauli,
New Delhi- 110030 (INDIA)

info@bharat6galliance.com

www.bharat6galliance.com