Bharat6G Alliance

Bharat 6G Alliance Whitepaper

SECURITY FOR 6G

October 2026

Bharat 6G Alliance Whitepaper

Security for 6G

October 2026

Executive Summary

6G is expected to build on 5G's capabilities and add new features by integrating AI, sensing, computing, and ubiquitous connectivity. These features will enable 6G be an intelligent and autonomous network that can support immersive applications and seamlessly connect physical and digital environments. However, this enhanced features also increases the threat landscape of 6G systems making them vulnerable to various type of security attacks. 6G systems are also envisioned as a generator of data that can enable many new applications like intelligent transportation system, urban planning, disaster management, and healthcare. As 6G system data can depend on user data, privacy issues also need to be carefully addressed.

6G deployment timeline is likely to overlap emergence of cryptographically relevant quantum computers. This requires that 6G to support post-quantum cryptography involving both symmetric and asymmetric and asymmetric mechanisms. There are several new security related issues both in the Radio Access Networks and Core Networks that needs to strengthen compared to the 5G networks or addressed afresh, like securing MAC-CE's, integrated sensing and communication. and security framework for collection and exposure of 6G system data.

As malicious attacks continue to evolve, 6G system should support mechanisms to collect events that will help to monitor to detection any malicious attacks early. This requires identification of relevant security events that need to be collected and analyzed.

In this whitepaper we study 6Gsecurity under the following six primary areas:

1. Cryptographic foundation of 6G
2. RAN security
3. Core network security
4. Interface security
5. Data collection for security monitoring
6. AI security.

For each area, we provide the security and privacy challenges and the potential solution directions to address them. Several of these potential solutions need further research to aid in their standardizations. We provide recommendations on standardization several 6G security issues that are of specific relevance to India like, adaption of hybrid post-quantum cryptography, SMS service, consent management, NTN, computing, security monitoring, AI agent security, that are of relevance in India. Further, we discuss activates ongoing in 3GPp and TSDSI on standardization of 6G security.

Table of Contents

Executive Summary 3

6G Security Architecture 6

1. Cryptographic Foundations for 6G 8

A. Post-Quantum Cryptography Migration 8

B. Evolution of Symmetric Cryptography for 6G 10

2. RAN Security 12

A. Message Protection (Confidentiality, Integrity, and Availability) 12

B. Key Management and Derivation 13

3. CORE NETWORK SECURITY 15

A. EXPOSURE 15

B. SERVICES (SMS, IMS, SENSING) 17

B.1 Short Message Services (SMS) 17

B.2 IP Multimedia Services (IMS) 18

B.3 Sensing (ISAC) 19

C. Data Framework 20

D. Authentication and Authorisation 21

D.1 Network Function Authentication and Authorization 21

D.2 Subscription Authentication and Authorization 23

4. INTERFACE SECURITY 24

A. UE-to-Core Network Security 24

B. Interconnect and Roaming 27

C. Security within the Core Network 28

5. Data Collection for Security Monitoring 30

A. General AI Security 33

B. Security of AI Agents in 6G 33

Recommendations: 35

Annexure: 37

1. 3GPP ongoing work 37

2. Overview of TSDSI Security Work for 6G 38

Acknowledgements 40

References 41

Introduction

Mobile communication networks have evolved from systems designed primarily to connect people into critical digital infrastructure supporting individuals, enterprises, industries and increasingly autonomous machines. 5G and 5G-Advanced have progressively expanded the scope of mobile networks, strengthening their ability to support a wider range of users, devices and applications with increasingly diverse performance and connectivity requirements.

6G represents the next stage in this evolution, driven by the expectation that connectivity will increasingly move from “anywhere” towards truly “everywhere” access, extending communication services to previously unconnected and underserved users and environments. Its development enhances capabilities established in previous generations while also introducing new technologies and service capabilities like Immersive Communication, Hyper-Reliable and Low-Latency Communication, Massive Communication, Ubiquitous Connectivity, AI and Communication, and Integrated Sensing and Communication (ISAC). Collectively, these scenarios support increasingly immersive and multi-sensory interactions, distributed computing and AI applications, ubiquitous connectivity, and sensing capabilities that can provide spatial information about connected and unconnected objects, their movements and their surroundings. The development of 6G is further guided by the overarching principles of sustainability, security and resilience, universal and affordable access, and ubiquitous intelligence. In addition to enabling new services, 6G is expected to improve overall system performance while addressing environmental, social and economic sustainability and supporting a smooth evolution from, and interworking with, existing 5G systems.

As communication networks become more deeply integrated with AI, computing, offering new serving based on sensing and non-terrestrial networks, the number of assets, interfaces and trust relationships requiring protection increases significantly. Exposure of 6G system data to applications such as intelligent transportation, urban planning and healthcare further expands the threat landscape. Security and privacy must therefore evolve alongside the system architecture, addressing both enhancements to existing security mechanisms and new risks introduced by emerging capabilities.

The security considerations for 6G consequently extend across the overall system architecture, the radio access network, UE-to-core network interactions, core network security and interfaces, end-to-end roaming, and security monitoring. At the same time, an important objective is to minimise the attack surface through lean and streamlined system design, including an appropriate set of functionalities, reduced use of multiple alternatives for the same functionality, and avoidance of excessive configuration complexity. These objectives align with Secure by Design principles and establish security, privacy, resilience and trust as integral considerations in the development of the 6G.

While academic researchers are actively studying the various security issues in 6G, International standardization bodies like 3GPP, GSMA, ITU-T are working on standardization of security of 6G [1][2][19]. Industry alliances and research consortia have also published their own 6G security visions [3][16]. At the national level, TSDSI have undertaken several new item proposals on 6G security. In this whitepaper, we will discuss various security and privacy issues that arise in 6G and potential solutions directions under consideration to address these issues. We will also highlight the research needed to narrow down on the solutions and the standardization considerations.

6G Security Architecture

The 5G security architecture defined in 3GPP TS 33.501 [33] establishes a comprehensive, layered framework to secure user privacy, access, and service-based core interactions. This 5G framework serves as a base architecture for evolution towards 6G. The core components of 5G security architecture are primary authentication, secondary authentication for external data networks, radio interface protection, non-access stratum signalling protection, and service-based interface security within the core. Primary authentication relies on 5G Authentication (5G-AKA) and Key Agreement or Extensible Authentication Protocol (EAP), executed between the User Equipment and the Home Network via the Access and Mobility Management Function and Authentication Server Function. A major advancement over previous generations is the default protection of permanent subscriber identities: the Subscription Permanent Identifier (SUPI) is encrypted into a Subscription Concealed Identifier (SUCI) using the home network's public key before transmission over the radio path. Key management follows a strict hierarchy where the master key stored in the Universal Subscriber Identity Module derives a unified anchor key, which in turn fuels distinct keys for Non-Access Stratum signalling, User Plane traffic, and gNodeB Access Stratum protection.

5G security architecture defines the security mechanisms spanning the Radio Access Network, Core Network, and interconnected interfaces. The RAN provides integrity and ciphering for control signalling and user plane data over the NR Uu interface, while key refresh procedures ensure forward and backward secrecy during handovers. Within the Core Network, the Service-Based Architecture employs Transport Layer Security and OAuth 2.0 authorization framework via the Network Repository Function, while the Security Edge Protection Proxy enforces mutual authentication, topology hiding, and integrity protection at interconnect interfaces between public land mobile networks. Interfaces connecting the UE to access network entities and core functions remain strictly segregated to contain potential breach domains.

Figure 1: Security Areas in 6G

The evolution toward a 6G security architecture is driven by radical shifts in the threat landscape and network paradigms. As wireless communications integrate post-quantum compute capabilities, sub-terahertz frequencies, distributed artificial intelligence, open radio access networks, and non-terrestrial networks, traditional centralized security boundaries become insufficient. Transitioning from 5G to 6G introduces complex security challenges across all structural domains. In the RAN, extreme data rates and massive cell disaggregation weaken centralized key distribution efficiency and heighten

vulnerability to physical tap attacks. In the Core Network, fully autonomous, AI-driven orchestration and microservice decay challenge conventional perimeter-based firewalls and static identity assertions. Furthermore, cross-domain interfaces face severe latency constraints, rendering heavy cryptographic handshakes impractical for mission-critical sub-millisecond communication links. Technical report 3GPP TR 33.801-01[30] highlights key study directions for 6G security, emphasizing post-quantum cryptographic resilience, zero-trust network function interaction, and dynamic trust management across heterogeneous system nodes.

To overcome these architectural bottlenecks, remedies centre on deploying lightweight, post-quantum resilient algorithms and embedding zero-trust mechanisms natively into every network function. Decentralized identity verification, automated adaptive key updates including handover cases, and unified continuous trust evaluation will ensure end-to-end isolation and resilience without compromising performance.

As the 6G security architecture continues to take shape, six key security areas have been identified to guide the ongoing study of security and privacy requirements (Figure 1). Together, these areas span the system architecture, radio access network, UE and core network interactions, authentication, network exposure, security monitoring, AI agents, data frameworks, and sensing. Work is ongoing within each area to identify the relevant security challenges, threats and potential security requirements for 6G. We group them into the following four major areas.

1. Cryptographic Foundations for 6G
2. RAN Security
3. Core Security
4. Interface Security

The above areas cover broadly how to secure for the 6G system. However, the system also needs mechanisms to proactively collect information on security events that are helpful in detecting the potential attack or investigate them. For this, standards also study which events needs to be monitored.

AI is proposed to be heavily utilized to enhance operation efficiency and support new features (AI for 6G). All the security issues that arise in generic AI systems need to be addressed in the 6G system. Additionally, 6G networks are expected to support the UE AI agents (6G for AI). This gives raise to new security challenges that are specific to the 6G systems. We will discuss these aspects under the following two major areas.

5. Data Collection for Security Monitoring
6. AI Security

The following sections deep dives into the security challenges, solution directions, research and standardization considerations for each of the areas.

1. Cryptographic Foundations for 6G

Quantum computers threaten to break or weaken modern cryptography. Shor's algorithm demonstrates that quantum computer can efficiently break the assumption on the hardness of the underlying mathematical problems, widely used public-key algorithms like RSA, Diffie–Hellman, and elliptic-curve cryptography. This could compromise asymmetric cryptography used in key exchange, digital signatures, and authentication. Grover's algorithm provides a smaller, quadratic speedup against symmetric cryptography and hash functions, reducing their effective security strength. The major response is Post-Quantum Cryptography (PQC), which replaces vulnerable public-key mechanisms with quantum-resistant algorithms.

This area identifies the issues and challenges in safeguarding 6G system against threat from quantum computer. We study cryptographic foundations required for trustworthy 6G systems, including migration to post-quantum cryptography, cryptographic agility, evolution of network-security protocols and adoption of authenticated encryption suitable for 6G radio and network interfaces. We discuss them under the following two sub areas.

A. Post-Quantum Cryptography Migration
B. Evolution of symmetric Cryptography for

A. Post-Quantum Cryptography Migration

The asymmetric cryptography is particularly vulnerable due to Shor's algorithm when cryptographically relevant quantum computers (CRQCs) become available. 6G networks are expected to operate well into the period when CRQCs can be a reality could threaten public-key cryptography currently used for key establishment and digital signatures.
To safeguard against these threats, migration to quantum-resistant cryptography should begin before CRQCs become available. Figure 2 summarizes why Shor's algorithm breaks asymmetric cryptography (used for key exchange and digital signatures) while symmetric cryptography remains safe against Grover's algorithm with a modest key-size increase. In the following, we discuss various security and privacy challenges to 6G networks due to cryptographically relevant quantum computer and potential solution approaches to safeguard them.

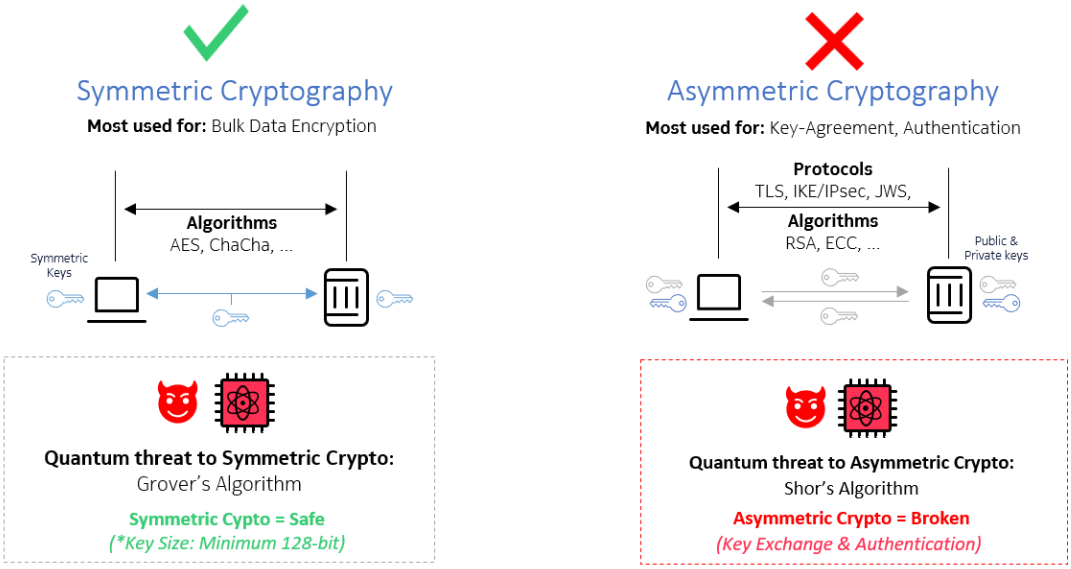

Figure 2: Quantum Threats to Symmetric and Asymmetric Cryptography

Security and Privacy challenge

- **Harvest Now, Decrypt Later:** Information encrypted using quantum-vulnerable public-key mechanisms may be collected and retained until quantum computation makes its decryption practical. The urgency of migration depends on the confidentiality lifetime of the information, the expected lifetime of the protection mechanism and the time needed to migrate the affected systems.
- **Compromise of authentication and trust:** Quantum attacks could undermine digital signatures and other public-key mechanisms supporting like Network and device authentication Certificate validation, Software and firmware integrity, Network-function communication, Inter-operator trust, External service, and API authentication. This could enable entity impersonation, fraudulent certificates, unauthorized network access or acceptance of malicious software.
- **Confidence in PQC:** The classical cryptography has evolved over time and are tested against various type of classical attacks. The same level of confidence is yet to emerge for the PQC. Though several PQC are standardized, it may take time to fully understand their resistance to all type of attacks including implementation related vulnerabilities [5][17].
- **Long infrastructure and credential lifetimes:** Telecom equipment, devices, embedded trust anchors and credentials can remain in operation for many years. Some deployed components may not be remotely upgradeable or may lack the processing, memory and storage required by new cryptographic mechanisms. Migration must therefore consider legacy interworking, hardware limitations and replacement of long-lived trust anchors.
- **Interoperability and downgrade risks:** A 6G service may span different operators, vendors, cloud providers, private networks, non-terrestrial networks and legacy mobile systems. These domains may migrate at different times. An attacker may also attempt to remove advertised PQC capabilities or force classical-only operation. Cryptographic negotiation must therefore be authenticated, downgrade-resistant and governed by explicit security policy.

Solution Directions

- **Crypto-inventory-driven migration:** The transition should begin with a continuously maintained inventory identifying all uses of quantum-vulnerable public-key cryptography across the 6G ecosystem. The inventory should include TLS, IKEv2/IPsec, certificates, certificate-management protocols, subscriber identity protection, software and firmware signing, vendor credentials and long-lived trust anchors.
- **Hybrid approach:** Use both classical and post quantum cryptographic algorithms till confidence in PQC is established for both key encapsulation mechanism (KEM) and digital signature (DSA). NIST has standardized several Module-Lattice based hybrid cryptographic algorithms for KEM and DSA. The hybrid algorithms can be supported in the 6G networks.
- **Introduce quantum-resistant subscriber identity protection:** Subscriber identifier-concealment (e.g. SUCI) mechanisms based on quantum-vulnerable public-key cryptography should be migrated to PQCA. This should be a distinct solution direction because identity protection has different message-size, provisioning, privacy and failure-handling requirements from ordinary TLS or IPsec communication
- **Cryptographic-agility requirements:** 6G protocols should avoid hard-coded dependencies on a single algorithm, parameter set or credential model. They can support of suite of hybrid algorithms with option to add new algorithms and remove vulnerable algorithms. Additionally, there should be a mechanism to transit from hybrid to PQC-only operations. Fallback to classical-only protection should be permitted only under explicit policy. It should be detectable, logged and, where appropriate, exposed to security-management functions.
- **Use Quantum Key Distribution (QKD) selectively as a complementary mechanism:** QKD may complement PQC for selected high-value links, such as national infrastructure, government communication, defence networks, financial data centres and critical backbone connections requiring unconditional security with full proof protection against eavesdropping.

It should not be positioned as a universal replacement for PQC because it requires specialized optical infrastructure, authenticated classical channels, key-management integration and operational monitoring.

Research and Standardisation Considerations

Research and standardisation should focus on the telecom-specific profiling, migration and validation of post-quantum mechanisms for 6G. Priority areas include:

- **Telecom performance evaluation:** Assess performance of hybrid and PQC-only algorithms for both KEM and DSA under realistic network conditions, including handshake latency, certificate-chain size, signalling fragmentation, processing, memory and energy consumption.
- **Protocol and credential profiling:** Define interoperable profiles for hybrid and PQ-only operation in TLS 1.3, IKEv2/IPsec, telecom PKI and subscriber identity protection, including parameter selection and failure handling.
- **Certificate and trust-anchor migration:** Evaluate PQC-only, composite and multiple-credential models, and define secure procedures for credential renewal, trust-anchor rollover and revocation.
- **Crypto-agility and downgrade protection:** Specify authenticated capability negotiation, policy-controlled fallback, algorithm deprecation and orderly transition from hybrid to PQC-only operation.
- **Implementation assurance and interoperability:** Establish common testing for side-channel resistance, fault attacks, secure key storage, multi-vendor interoperability, roaming, constrained devices and phased legacy migration.

Coordinated testbeds and interoperability trials will be essential to validate complete telecom procedures and achieve quantum-safe 6G without fragmentation, silent fallback or disproportionate impact on low-cost and constrained devices

B. Evolution of Symmetric Cryptography for 6G

When CRQCs are a reality, Grover's algorithm offers quadratic improvement in the complexity of brute force key search of symmetric cryptographic. This roughly translates to a symmetric key length of n to be only as affective of that of key length n/2 for the quantum computers. To ensure the same level of security that the modern symmetric key algorithms offer against classical computers, higher key lengths need to be considered in presence of CRQCs. The need for higher key lengths also applies to crypto modules used in integrity protection and authentication verification. Two complementary enhancements are particularly relevant in Symmetric Cryptography of 6G:

- Transition to 256-bit symmetric cryptographic algorithms
- Adoption of Authenticated Encryption with Associated Data, or AEAD

The need for confidentiality and integrity protection depends on the threat perception and whether the devices have the required hardware and software capabilities. Also, the higher level of key-lengths and the encryption may affect performance ins some case. This requires defining various protection-modes (confidentiality only, integrity only, or both) and the impact of each mode on the real performance.

Security and Privacy challenge

- **Hardware and implementation impact:** The introduction of 256-bit algorithms may affect UE chipsets, baseband processors, radio equipment, cryptographic accelerators, secure elements and software libraries.
- **Algorithm and protection-mode negotiation:** With combined-mode algorithms, the UE and network need to agree on both the cryptographic algorithm and the required protection mode. The possible modes include, Combined confidentiality and integrity, Integrity only, Confidentiality only, no protection, where explicitly permitted. An attacker may attempt to modify capability information, force selection of a weaker algorithm or disable integrity protection. The selected algorithm and protection mode should therefore be cryptographically bound to the security context and protected against replay, modification and downgrade
- **Key derivation and separation:** AEAD uses a single key for combined confidentiality and integrity protection. Compromise of a key in one protocol domain from affecting another domain. The key hierarchy should also ensure that mobility, context transfer or recovery does not cause key reuse across different security contexts

Solution directions

- **Support 256-bit symmetric protection:** The 6G security framework should support 256-bit input keys for NAS signalling, RRC signalling, and User-plane traffic
- **Independent key derivation:** The 6G security framework can support independent encryption and integrity keys for NAS protection, RRC protection, and User-plane protection.
- **Interoperability:** A minimum interoperable algorithm profile can be defined to avoid deployment fragmentation. Additional algorithms may be supported according to regional, regulatory or deployment-specific requirements.
- **Support for different protection modes:** The applicable cryptographic mechanism can support Combined confidentiality and integrity, Integrity-only, Confidentiality-only protection, or Partial confidentiality with full integrity. This approach supports the different protection requirements of NAS, RRC and user-plane traffic within a common cryptographic framework. The mature technical direction is to use NCA for combined and integrity-only protection, while NEA provides confidentiality-only protection.
- **Secure failure and fallback behaviour:** Failure handling should avoid providing detailed cryptographic information to an attacker and should not allow forged traffic to repeatedly trigger expensive recovery procedures Where 256-bit or combined protection cannot be negotiated, fallback should occur only under explicit policy. It should be authenticated, observable, auditable and protected against attacker-induced downgrade.

Research and Standardisation Considerations

- **Algorithm profiles:** Define the minimum 256-bit algorithm set and optional profiles for different 6G device, network, and assurance categories.
- **Protection-mode integration:** Specify combined, integrity-only and confidentiality-only protection for NAS, RRC and user-plane traffic.
- **Performance and interoperability:** Assess throughput, latency, packet overhead, energy consumption, mobility, legacy interworking, and multi-vendor operation.
- **Implementation assurance:** Establish testing for side channels, fault attacks, incorrect tag verification, key leakage, and unauthorized release of plaintext.

Testing should validate complete NAS, RRC and user-plane procedures under realistic radio, network, and device conditions, rather than evaluating cryptographic algorithms only in isolation

2. RAN Security

This area focuses on (refer to Fig. 2) protecting the radio access network, including its architecture, protocols, interfaces, and procedures. It also addresses security implications arising from mobility, state transitions, and interactions between the radio network, UEs and the core network [7][8][30]. At high level, this area is divided into two parts:

A. Message protection
B. Key management

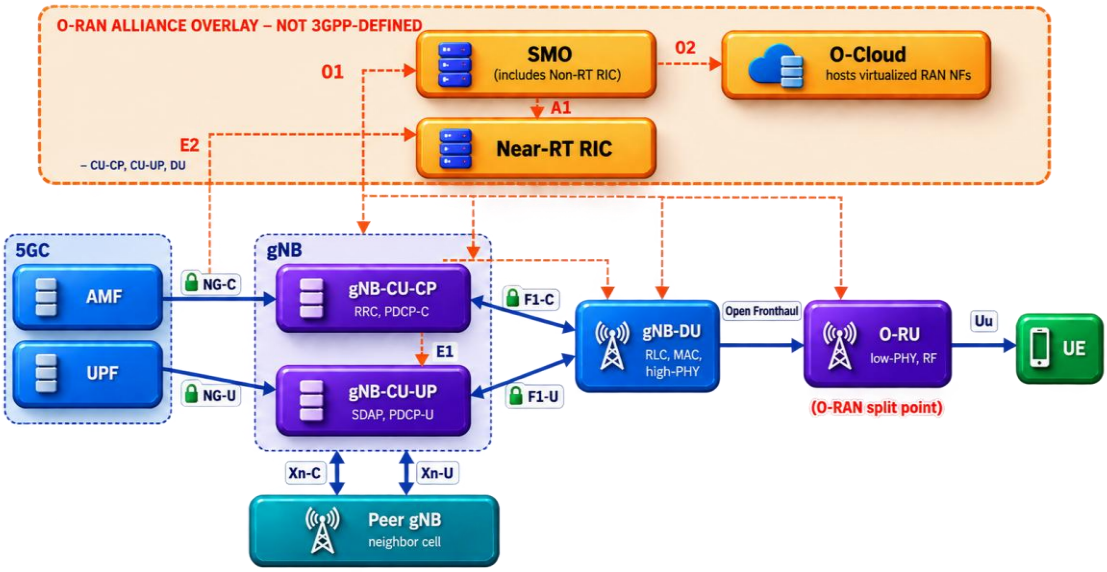

Figure 3: 6G RAN Security

A. Message Protection (Confidentiality, Integrity, and Availability)

This section addresses protection of RRC, MAC signaling, and user data against interception, modification, and denial-of-service attacks throughout the protocol stack.

Security and Privacy Challenges

The critical vulnerabilities within the physical, architectural, and signaling domains that jeopardize the protection of 6G RAN messages include,

- **Over-the-Air (OTA) & Radio Link Vulnerabilities:** Air-interface control messages are susceptible to active radio jamming, spoofing, unauthenticated side-channel eavesdropping, and rogue base station impersonation [5][22].
- **Signaling Integrity Gaps:** Critical lower-layer control procedures, specifically MAC Control Elements (MAC CEs) and RLC Transport Blocks (when AS security is not activated), are at risk of eavesdropping, malicious injection or alteration during transmission [22, 23].

- **Physical Security Exposure:** Disaggregated radio nodes (CU-DU Split architecture), deployed in unstaffed locations, create physical access points for signal manipulation and data interception.

Solution Directions

Following are the emerging cryptographic and defence frameworks tailored to the stringent sub-millisecond requirements of the RAN.

- **PHY-Layer Security & Noise Injection:** Utilizing Channel State Information (CSI) for secure transmissions and injecting low-overhead differential privacy noise into MAC/PHY scheduling vectors prevents data poisoning in federated beamforming models.
- **Low-Latency PQC & OTA Integrity**: Customizing lightweight Post-Quantum Cryptographic (PQC) primitives to encapsulate payloads directly within 3GPP MAC CE and RLC Transport Block structures secures control-plane signalling [17, 23].
- **Signal Auditing**: Deploying hardware-accelerated AI/ML agents within the gNB Distributed Unit (gNB-DU) continuously audits PHY IQ data streams for RF fingerprint anomalies, jamming, and signal spoofing.
- **Mobility Threat Mitigation**: Lower-layer predictive algorithms monitor mobility state transitions across local scheduling queues to detect anomalous handover requests and prevent ping-pong signalling exploits.

Research and Standardisation Considerations

This subsection highlights critical standardisation considerations and operational trade-offs that must be addressed to deploy effective 6G RAN message protection.

- **Strict Execution Constraints:** 3GPP Working Group SA3 is placing explicit emphasis on the sub-millisecond constraints of the PHY, MAC, and RLC sublayers when addressing vulnerabilities like OTA message manipulation.
- **OTA Integrity Standardisation:** Discussions are exploring standardizing lightweight integrity protection and ciphering mechanisms directly within MAC CE payloads and RLC header extensions.
- **AI/ISAC Policy impacts:** Standards aim to establish uniform verification frameworks for PHY-layer AI/ML beamforming models and privacy-preserving policies for Integrated Sensing and Communication (ISAC) workflows.
- **Operational RRC Impacts:** Enforcing per-packet integrity verification and cryptographic handshakes can disrupt HARQ timing, cause RLC buffer bloat, and impair real-time beamforming adaptation.

B. Key Management and Derivation

This section focuses on the secure establishment, update, and transfer of RAN security keys required for authentication and cryptographic operations across 6G RAN functions (RRC, PDCP). The emphasis is on ensuring forward-secure key derivation isolated from infrastructure compromise and optimizing key updates for low-latency mobility events.

Security and Privacy Challenges

The threat landscape targeting 6G RAN key hierarchies, focusing on vulnerabilities during mobility and within shared microservice execution environments includes,

- **Mobility & Control Transfer Security Gaps:** Risks are introduced during rapid context transfers over Xn and F1 interfaces, where target cell preparation and re-keying procedures can be exploited.
- **Context Transfer Exploitation:** Unsecured control transfers can lead to handover signaling manipulation, service hijacking, or ping-pong instability during inter-DU and inter-CU handovers.
- **Expanded Topologies:** Key management hierarchies face challenges in securing expanded access topologies, Multi-Access Edge Computing (MEC) infrastructure, and slice isolation across disaggregated units.

Solution Directions

The architectural defences, such as forward-secure hierarchies and TEE/Physical Layer Security (PLS)-based isolation, necessary to ensure keys remain secure and efficient under 6G operating paradigms includes,

- **Forward-Secure Key Hierarchies:** Utilizing zero-RTT forward-secure key hierarchies and Xn/F1 context bound-checking for hitless handover re-keying.
- **Fine-Grained Transport Security:** Deploying IPsec and Network Domain Security (NDS/IP) protocol suites paired with hardware-enclosed Trusted Execution Environments (TEEs) for isolated key derivation.
- **Hardware-Backed Attestation:** Utilizing TEEs for hardware-backed early target cell attestation ensures the integrity of the target node before key transfer.

Research and Standardisation Considerations

This subsection discusses research priorities and standardisation considerations targeting quantum-resistant and zero-trust key management within the 6G RAN.

- **Normative Mobility Key Hierarchies**: Defining normative zero-RTT forward-secure key derivation hierarchies for hitless inter-DU/CU handovers over Xn and F1 interfaces.
- **Zero-Trust Interface Architectures:** Standardizing zero-trust reference architectures across disaggregated 3GPP interfaces, including F1, Xn, and NG [6][9].
- **Low-Latency Attestation Protocols:** Explorations are underway regarding hardware-backed remote attestation protocols operating within TEEs to verify lower-layer microservice integrity during rapid cell context transfers.

3. CORE NETWORK SECURITY

6G network core will continue to support traditional services like SMS, IMS, MMS, network slicing, mobile broadband, positioning, tracking, and will be upgraded to support new features like sensing, computing, and other AI enabled services. Several new Network Functions (NFs) will be introduced to support the new features while improving the capabilities of the exiting NFs. The security of each of the services and the communication between the NFs needs to be strengthened with a robust authenticated and authorized mechanism. Additionally, the rich data generated in the 6G system through the services and the NFs need to be securely collected and exposed while preserving user privacy. We study various aspects of the core network security under the following four subgroups.

A. Exposure
B. Services (SMS, IMS, Sensing)
C. Data Handling (Data Framework)
D. Authentication and Authorization

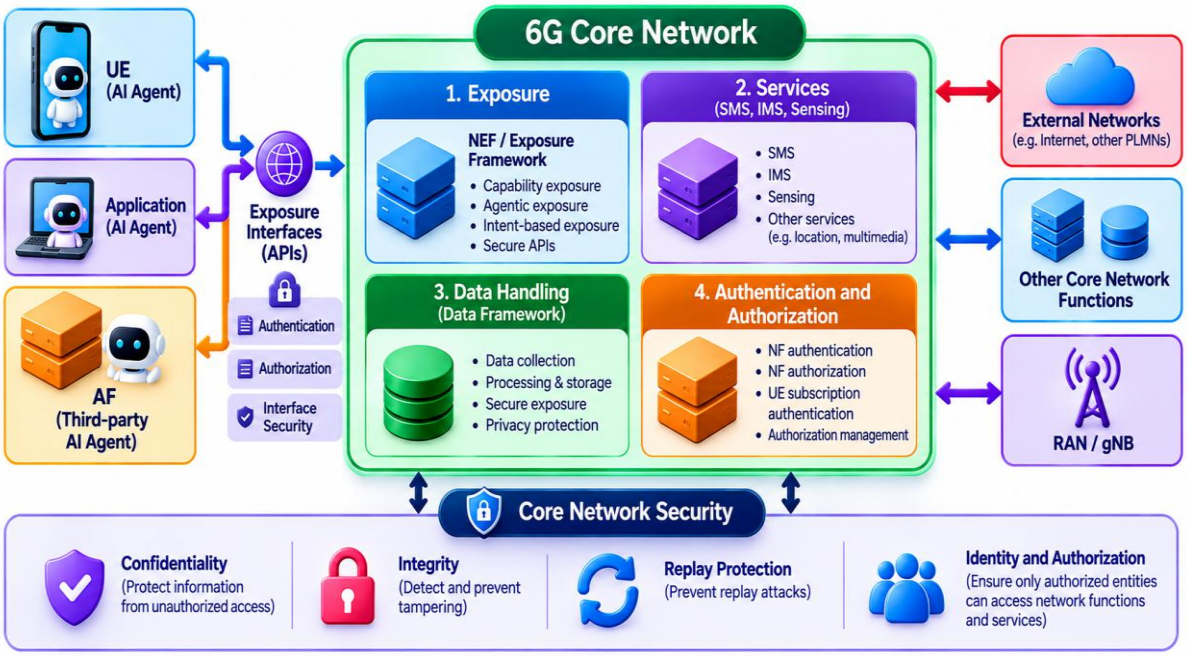

Figure 4: 6G Core Network

A. EXPOSURE

6G is expected to support the exposure of network capabilities to UEs, applications, and third-party entities through a common exposure framework [4][5][31]. This area covers the security of the common exposure framework, exposure interfaces for both AI and non-AI use cases, and enhancements to CAPIF for new exposure mechanisms.

As exposure becomes more dynamic and increasingly involves intent-based interactions and AI agents, security needs to address not only the identity of the API invoker but also the authorization context, requested capabilities, delegation, and protection of the exposure interfaces.

Security and Privacy Challenges

- **Authentication and authorization of exposed capabilities:** Improper authentication may allow an entity to impersonate another when requesting exposed network capabilities, such as QoS functionalities, while insufficient authorization may allow access to those capabilities beyond the permitted scope. For capability exposure to UEs and application endpoints, the study also considers authorization changes and revocation, as well as the protection of exchanged information.
- **Protection of exposure interfaces:** Exposure interfaces need protection against unauthorized observation, modification, and injection of messages. Confidentiality and integrity are particularly important when exposed capabilities involve network control information or service-related metadata.
- **Third-party AI agents as API invokers:** AI agents introduce security considerations that are not fully addressed by exposure mechanisms designed for conventional API invokers. These include agent onboarding, identification, authorization, capability handling, delegation, and access to AI-oriented services. An unauthorized or malicious AI agent could attempt to access sensitive information or network resources beyond its permitted scope.
- **Agentic exposure through the Core Network:** Agentic exposure through the NEF introduces additional concerns around authentication, authorization, and interface security. Threats include impersonation of a legitimate AF AI agent, access beyond an agent's authorized scope, intent, role, or delegated permissions, and modification, injection, or observation of messages exchanged with the Core Network.
- **Intent-based exposure:** Intent-based exposure introduces a higher-level form of interaction in which an entity requests network capabilities through an intent. Inadequate authentication, authorization, or interface protection could enable resource abuse, unauthorized access, information leakage, impersonation, eavesdropping, message injection, or message alteration. The appropriate granularity of authorization remains an open study item.

Solution Directions

For most of these key issues, the study has not yet defined solutions or agreed security requirements; the directions below follow from the identified threats rather than from TR-adopted requirements. Intent-based exposure is the exception, where the study has already identified specific potential security requirements.

- **Strong authentication and authorization:** Exposure frameworks should establish the identity of entities requesting network capabilities and ensure that requested services remain within the authorized scope.
- **Capability and context-aware authorization:** Authorization should consider the capabilities being requested and, where applicable, the relevant authorization, role, or delegated permissions. Changes to authorization should also be reflected in ongoing service access, including appropriate revocation.
- **Secure exposure interfaces:** Exposure interfaces should provide appropriate confidentiality and integrity protection. For intent-based exposure, the current study additionally identifies replay protection as a potential security requirement.
- **Security for third-party AI agents:** Security procedures should account for the onboarding and identification of AI agents, their authorization to invoke exposed capabilities, capability handling, and delegation. The trust context used for granting access should not rely solely on capabilities or trust information self-declared by an AI agent.

- **Protection of agentic exposure:** Agentic interactions between AF AI agents and the Core Network should incorporate authentication, authorization, and secure communication appropriate to the exposure architecture, while restricting an agent's access to its authorized scope, intent, role, and delegated permissions.
- **Secure intent-based exposure:** Intent-based exposure should support mutual authentication of communicating entities, authorization of intent-based requests, and confidentiality, integrity, and replay protection for the interfaces used for such exposure. These are identified as potential security requirements in the current study.

Research and Standardisation Considerations

- **Common exposure security framework:** Define security requirements for the common exposure framework and its interfaces while maintaining consistent security principles across AI and non-AI exposure scenarios.
- **AI-agent-aware exposure security:** Further study is needed to define security requirements for third-party AI agents acting as API invokers, particularly for onboarding, identification, authorization, capability handling, and delegation. The potential security requirements for this key issue remain TBD in the current TR.
- **Agentic exposure via NEF:** Security requirements for agentic exposure, including the relationship between agent identity, authorization scope, intent, role, and delegated permissions, require further study. The potential security requirements for this key issue are currently TBD.
- **Intent authorization granularity:** The appropriate granularity for authorization of intent-based requests remains for further study. Future standardisation should further determine the appropriate authorization granularity and how intent-based requests are authenticated and authorized within the exposure framework.
- **Alignment with 6G architecture:** Exposure security needs to remain aligned with the ongoing architectural work in TR 23.801-01[31] and TR 23.801-02[32]. Existing security mechanisms should be reused wherever feasible, while addressing security requirements introduced by new exposure models.
- **Separation of study-stage requirements:** The current TR contains a mixture of identified potential requirements and open/TBD items. Subsequent standardisation should distinguish established security requirements from areas that remain under study as the 6G exposure architecture evolves.

B. SERVICES (SMS, IMS, SENSING)

This area focuses on the protection of SMS, IMS and Sensing services, including issues related to their architecture, signalling flow, and procedures.

B.1 Short Message Services (SMS)

The security requirements for SMS services, critical baseline communications legacy mechanism for point-to-point data, legacy alerts, and Two-Factor Authentication (2FA) verification, defined by 3GPP TS 23.040 [37] specify the legacy point-to-point Short Message Service (SMS) architecture, routing principles, and payload transfer protocols.

Security and Privacy Challenges

The multi-domain interworking and legacy network constraints driven security and privacy vulnerabilities of SMS services include,

- **Sender Information Spoofing:** Traditional SMS lacks native cryptographically bound originator verification, enabling malicious actors to perform SMS spoofing via fake Short Message Service Centers (SMSCs) or manipulated MAP/SMPP headers.
- **IMSI/MSISDN Exposure & Interception:** Legacy Signaling System No. 7 (SS7) and Diameter vulnerabilities allow eavesdropping, SIM swapping, and interception of one-time passwords (OTPs).
- **Gray-Route Traffic & Spam:** Unregulated routing channels facilitate unverified Application-to-Person (A2P) message injection, eroding trust and facilitating phishing campaigns.

Solution Directions

Following are cryptographic solution directions for security and privacy vulnerabilities of SMS services,

- **Cryptographic Sender Information Verification:** Integrating digital signatures or public key infrastructure (PKI) signatures over NAS containers directly from the originating UE/NW node to ensure payload and identity integrity.
- **3GPP Core Security Filters & DLT/STIR/SHAKEN Paradigms:** Implementing SS7/Diameter Firewalls (3GPP FS.11/FS.19), Distributed Ledger Technology (DLT) registries (e.g., India's TRAI DLT platform), and framework extensions for caller/sender identity verification.
- **Authentication-Centric Carrier Verification:** End-to-end payload signature validation prior to delivering A2P messages to the target mobile device.

Research and Standardisation Considerations

The academic and industry technology considerations include,

- Investigating security enhancements for messaging, targeting explicit Sender ID verification mechanisms over Service-Based Interfaces (SBI) in 5G/6G core networks.
- Zero-trust SMS delivery pipelines, automated ML-based smishing detection at the gNB layer, and lightweight cryptographic identity attestations for legacy mobile stacks.

B.2 IP Multimedia Services (IMS)

The security requirements for IP Multimedia Subsystem (IMS), which serves as the architectural standard for session-based voice, video, and rich multimedia services over IP-based cellular networks, defined by 3GPP TS 23.228[36] establishes the general architecture and functional signalling flows required to deliver multimedia services across heterogeneous radio accesses.

Security and Privacy Challenges

The IP domain interworking security and privacy challenges for IMS services include,

- **SIP Signaling Vulnerabilities:** SIP is prone to Distributed Denial of Service (DDoS), Session Hijacking, and Registration Spoofing attacks across untrusted IP interconnects.
- **User Identity Privacy:** Exposure of explicit SIP URIs (e.g., sip:user@domain), IP addresses, and User Equipment (UE) capabilities across unencrypted control signals.

- **Cross-Domain Trust Exploitation:** Insecure IPX/NNI (Network-to-Network Interfaces) allow rogue peer networks to inject unauthorized media traffic or track user mobility patterns.

Solution Directions

The interworking trust and signaling related security and privacy challenges can be overcome through solution in one of the following directions,

- **AKA and IPsec Enforcements:** Mandating IMS Authentication and Key Agreement (IMS-AKA) under **3GPP TS 33.203** [35] alongside IPsec Encapsulating Security Payload (ESP) tunnels between the UE and the P-CSCF, as specified for 3GPP IMS access.
- **SCONE & NNI Security Protocols:** Employing TLS-encrypted SIP interfaces and Security Gateways (SEG) at border control entities (IBCF/TrGW) to ensure signaling confidentiality and payload integrity.
- **Privacy-Preserving Headers:** Utilizing anonymized headers (P-Preferred-Identity / P-Asserted-Identity) and temporary session identifiers to shield real subscriber details from unauthorized third parties.

Research and Standardisation Considerations

The considerations for protecting IMS services include,

- Service-Based Architecture (SBA) transformations for IMS control functions, aiming to align traditional SIP signaling with modern RESTful APIs.
- Zero-Trust IMS frameworks, quantum-safe TLS/IPsec handshakes, and AI-driven SIP anomaly detection systems.

B.3 Sensing (ISAC)

The security requirements for Sensing/ISAC services, that leverages millimetre-wave and sub-6GHz radio environments to simultaneously deliver communication and target/environment detection, specified in 3GPP TR 38.901 [38] (ISAC channel extensions) defines geometry-based stochastic channel models incorporating radar target scattering points, bistatic clutter, and target propagation dynamics [13][14][15].

Security and Privacy Challenges

The ambient environment exposure and handling of sensitive information poses following security and privacy challenges,

- **Sensitive information:** Unauthorized radio sensing can expose private physical indoor locations, track unauthorized individuals, or reveal sensitive infrastructure layouts [13][14].
- **Adversarial Spoofing & Jamming:** Malicious target reflection injection or active radio jamming can disrupt range-Doppler estimation, target detection, and environment mapping [15].
- **AI/ML Model Evasion:** AI/ML-driven sensing pipelines are vulnerable to adversarial radio frequency perturbation attacks designed to mislead radar classification algorithms.

Solution Directions

- **AI/ML-Enabled Radio Interfaces:** Leveraging deep neural networks (DNNs) and reinforcement learning for joint waveform design, automated noise subtraction, and adaptive beam alignment.
- **MIMO Beamforming & Interference Management:** Implementing spatial Null-Steering and multi-cell coordinated beamforming to block sensing signals from entering unauthorized physical zones.
- **Resource Allocation & Target Imaging Constraints:** Dynamic radio-resource management (RRM) that cryptographically schedules sensing slots while interleaving communication symbols to prevent unauthorized target signature extraction.

Research and Standardisation Considerations

- Defining explicit use cases, service requirements, and architectural frameworks for 5G-Advanced and 6G network-integrated sensing.
- Physical-layer security (PLS) for ISAC, deep-learning-based environment reconstruction, low-complexity target imaging algorithms, and Privacy-Preserving Radio Resource Management.

C. Data Framework

As 6G is poised to support several new services with a well-defined framework for data collection and exposure. 6G system data includes data generated by various services, interfaces, user activity, and network functions which need to be collected, processed, stored, and retrieved while ensuring security and privacy aspects. Further, data could be collected from multiple sources requiring mechanisms to support federated learning and distributed computing.

Security and Privacy Challenges

- **Sensitive information exposure:** Network functions generate data containing subscriber identities, location information, communication patterns, session details, and service usage. Unauthorized access to 6G system data can leak subscriber-related information. Privacy risks when combining datasets from different network functions.
- **Data security and integrity:** Data collection introduces additional interfaces and storage points. The attackers can compromise data collection agents and inject false measurements. Attackers can attempt for unauthorized access to data and manipulate it leading to wrong analytics.
- **Data ownership and governance:** Data may reside in multiple geographical locations and owned by different operators. The data collection needs to comply with the local laws and data sharing policies must be clearly agreed.
- **Consent management:** As 6G system data can reveal user activity information, user consent management can be challenging. Additionally, the 6G system needs to ensure that the only necessary information is collected.

Solution Directions

- **Federated learning and distributed analytics:** Data is generated at multiple sources in 6G system. Instead of transferring data in bulk to a central location, learning can be done in distributed fashion keeping the data within its administrative domain.

- **Privacy-preserving data collection:** To avoid any leakage of information, data minimization policy can be applied where only the minimal data required for the application is revealed after anonymization it and removing any subscriber related information (e.g., SUPI, GPSI, location).
- **Data integrity and provenance:** Use of digital signatures, timestamps, and sequence numbers for collected records. Identification of data locations and transformation. Identification of inconsistent and manipulated measurements.

Research and Standardisation Considerations

- User data anonymization to ensure any exposure of 6G system data or any information derived from it, does not reveal user specific information.
- Mechanism for secure collection, storage, processing, and transfer of data.
- Mechanisms for operators to collect consent as per local governing laws.

D. Authentication and Authorisation

Authentication and authorization establish who, or what, is communicating with the 6G Core Network, and what it is allowed to do. We distinguish the authorization and authentication aspects in the Core Network based on who is requesting the services. The requester of service could be Network function withing the core network or an UE accessing 6G system services on its subscription. We discuss these issues in the following two

A. Network Function Authentication and Authorization
B. UE Subscription Authentication and Authorization

D.1 Network Function Authentication and Authorization

In the 5G Core Network, network functions establish each other's identity and confirm that a requested service is one they are permitted to use, before any service is provided [30]. The 6G security study examines whether this model holds up as Core Network deployments change, particularly in cloud environments and in indirect and interconnect communication.

Security and Privacy Challenges

- **Separation of authentication and authorization:** In cloud deployments, the point where a network function's identity is established and the point where its actual service logic runs are often different workloads — for example, a load balancer, gateway or sidecar handles the secure connection while a separate instance implements the function itself. When an intermediary such as a Service Communication Proxy (SCP) sits between two network functions, the secure connection is also only protected hop by hop, not end to end, between the requesting and the responding function. This separation increases the number of potential entry points for an attacker, complicates monitoring, and can lead to inconsistent access control if the two points are not securely linked.
- **Replay of authorization proofs:** A network function cannot always verify that whoever is presenting proof of authorization is the same function that proof was originally issued to, particularly in indirect communication and interconnect scenarios. Because this proof is not bound to the sender in 5G, one that has been intercepted or leaked can be reused by another authenticated party.
- **Reach of authorization:** Authorization is meant to be restricted to an intended recipient, but when that recipient is expressed as a whole category of network function rather than a specific

one, a single authorization can end up covering a much larger group of functions than intended, weakening the protection this restriction is meant to provide.

- **Confidentiality of the authorization exchange:** End-to-end mutual authentication between the requesting function and the function that grants authorization is not always achievable, particularly through an SCP and in roaming. Intermediate entities on the path can then be exposed to the authorization exchange, or in some cases could forge a request using details of a previous one.
- **Fit of the authorization model for 6G:** 5G supports two ways for a network function to obtain and check service authorization: a centralized approach, where a designated function issues an authorization token that the receiving function then validates itself, and a simpler, locally configured approach that does not need a dynamic exchange at all. The study is examining whether either approach, or the wider service-based framework they both sit within, remains suitable as the 6G Core Network architecture evolves — this work is itself provisional on a broader 6G architecture decision that has not yet been made [30][33].

Solution Directions

- **Linking identity to authorization:** Candidate approaches aim to bind a network function's authenticated identity to its authorization more directly, independent of where the underlying secure connection terminates. Some proposals have the requesting function itself prove possession of its own key at the point of the request; others keep today's split model but add a verifiable link between the authentication and authorization points.
- **Binding authorization to the sender:** Candidate approaches aim to tie an authorization proof to the specific function it was issued to, so that a copied or intercepted proof cannot be reused by another party.
- **Narrower reach of authorization:** Candidate approaches restrict authorization to a smaller, more specific group of functions, letting the granting function choose the narrowest reach that still fits the deployment — for example an NF Set rather than a whole NF type, or a reach selected dynamically from factors such as the target NF service, network slice, network slice instance, or the operator's own policy.
- **Protecting the authorization exchange:** Candidate approaches require end-to-end protection between the requesting function and the function that grants authorization wherever this is achievable, and limit deployment options that would otherwise expose the exchange to an intermediary.
- **Authorization architecture:** A candidate approach considers letting individual network functions, or small groups of them, grant authorization locally rather than relying on a single central function for the whole Core Network.

Research and Standardisation Considerations

- Evaluate the candidate approaches for linking network function identity to authorization and converge on a consistent mechanism for direct and indirect communication.
- Define a mechanism to bind authorization proofs to the sender, to prevent replay in indirect communication and interconnect scenarios.
- Decide the appropriate reach for authorization in the 6G Core Network.
- Define end-to-end protection requirements for the authorization exchange across indirect communication models and roaming.
- Decide whether the 6G authorization architecture keeps a centralized model, adopts a distributed or local model, or supports both.

D.2 Subscription Authentication and Authorization

The security study examines how the existing 5G authentication and key-agreement framework can be carried forward to 6GS while addressing new access architectures, mobility conditions and service-specific authorization. This includes authentication over both 3GPP and non-3GPP access, re-authentication during mobility, subscriber identifier privacy, protection of long-term credentials, secondary authentication with external data networks, and network-slice-specific authentication and authorization [30].

Security and Privacy Challenges

- **Primary authentication and key agreement:** 5G already runs a mutual authentication and key agreement procedure between the UE and the network when the UE first connects. The study is examining the security aspects of this procedure for 6G, including whether it needs enhancement [18].
- **Untrusted non-3GPP access:** In 5G, access through an untrusted non-3GPP network, such as WLAN, relies on a defined security model where signalling security terminates at the mobility management function and access security is anchored separately. For 6G, several architectural options for non-3GPP access are still under study, so the 5G security assumptions and procedures cannot be reused without re-evaluation.
- **Further topics within scope:** Re-authentication during mobility, subscriber identifier privacy, long-term credential storage and processing, secondary authentication with an external data network, network-slice-specific authentication and authorization, and authentication for localized service access are all identified as within scope, but their specific threats and requirements have not yet been elaborated in the study.

Solution Directions

- For primary authentication and key agreement, the 6G security study takes the existing 5G procedure as the interim basis, pending further study of any 6G-specific enhancements.
- For untrusted non-3GPP access, and for the further topics listed above, no solutions have yet been documented; this work depends on the corresponding 6G architecture decisions.

Research and Standardisation Considerations

- Complete the security analysis for primary authentication and key agreement and determine whether 6G requires enhancements beyond the 5G baseline.
- Define the security architecture for untrusted non-3GPP access once the corresponding 6G architecture options are narrowed.
- Elaborate the threats and requirements for re-authentication during mobility, subscriber identifier privacy, long-term credential storage and processing, secondary authentication, network slice-specific authentication and authorization, and localized service access authentication.

4. INTERFACE SECURITY

6G security needs to address communication between the User Equipment (UE) and the Core Network, communication within the Core Network, and communication between networks for interconnect and roaming. In 5G, these correspond to Non-Access Stratum (NAS) signalling between the UE and the Access and Mobility Management Function (AMF) over the N1 reference point, service-based interfaces (SBIs) between network functions, and the N32 interface between the Security Edge Protection Proxies (SEPPs) of different PLMNs [27][33]. The corresponding 6G reference points have not yet been defined, as the 6G architecture is still under study [31].

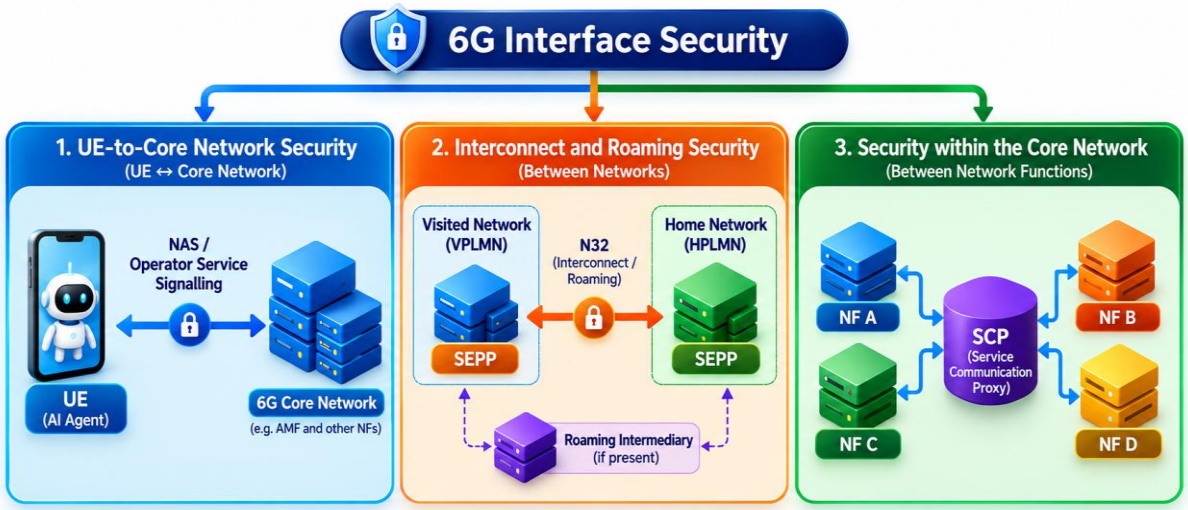

Figure 5: Interface Security

This section focuses on protecting the communication and the information exchanged: confidentiality, integrity and replay protection, security contexts and keys, and protection across network and domain boundaries. Authentication and authorization of UEs, network functions and other entities are addressed in Section 3.4. The 6G security study addresses these topics primarily under UE-to-Core Network security and Core Network, interconnect and roaming security, both of which build on the 5G security architecture in TS 33.501[33].

This area contains three parts (Figure 5):

A. UE-to-Core Network Security
B. Interconnect and Roaming
C. Security within the Core Network

A. UE-to-Core Network Security

Communication between the UE and the Core Network carries signalling for access, mobility, session management and other network services. The 5G NAS security requirements, excluding algorithm requirements, are used as the baseline for 6G. The security study takes the following as the baseline:

- The UE and the Core Network support confidentiality, integrity and replay protection of NAS signalling.
- Integrity protection of NAS signalling is mandatory, except at least for unauthenticated emergency calls.

The challenges below concern keeping these protections as NAS functionality, operator-service signalling and interworking change.

Security and Privacy Challenges

- **NAS security termination:** In 5G, the AMF is the primary NAS security termination point, and communication between the UE and other network functions is typically mediated by the AMF. SA2 is studying two models: a single NAS mobility-management termination point, and modular NAS, in which different NAS functionalities can terminate in different Core Network functions. For both models, the security study considers NAS algorithm selection, key activation, protection of NAS signalling and handling of security contexts. Confidentiality, integrity and replay protection of NAS signalling are needed whether there is one termination point or several. The associated security threats remain under study as the 6G architecture evolves [30][31].
- **Generic UE-to-Core Network interactions:** SA2 is studying generic ways to support operator services, such as service discovery and operator-service signalling. This signalling may be carried over the control plane, the user plane, a mix of the two, or a new plane, and it needs confidentiality, integrity and replay protection. Insufficient protection could expose operator-service information or allow signalling to be modified or replayed. Where NAS is used, this protection needs to be coordinated with NAS security to avoid gaps, duplicated protection or inconsistent security handling.
- **Parameter transfer between the UE and the Home Network:** In 5G, Steering of Roaming (SoR) and UE Parameters Update (UPU) both allow the Home Network to send integrity-protected information to the UE, but they were defined as separate procedures. As a result, the Authentication Server Function (AUSF) keeps a UE security context only for these procedures, and the security endpoint (AUSF) is not the same as the signalling endpoint, the Unified Data Management function (UDM). The study also identifies procedures in which end-to-end integrity protection between the UE and the Home Network is not currently provided, for example when the UE updates its location privacy settings in the UDM. 6G needs a generic approach that protects parameter transfer in both directions, including secured packets from the Home Network to the UICC.
- **Interworking:** When a UE moves between 6GS and existing mobile systems, its security contexts need to be handled correctly. The security requirements, and how security contexts are mapped or derived between systems, remain under study.
- **NAS identifier privacy:** In 5G, temporary identifiers assigned by the network limit how far a UE can be exposed, tracked or linked. This protection needs to be kept for both the single and the multiple termination-point models.
- **NAS key separation:** In 5G, a new AMF key (K_AMF) can be derived from the previous one when the serving AMF changes. This provides backward security only: knowledge of a K_AMF can allow the subsequent keys to be derived until a new primary authentication is performed. As a result, compromise of an AMF security context can affect subsequent NAS security contexts. Performing primary authentication more often would avoid this, but it increases load on the UDM and signalling in the network and at the UE. The study considers key separation between AMFs, to limit the impact of a compromised key to the corresponding security context. The study also considers where the security anchor function is placed, and whether co-locating it with the AMF, as in 5G, provides a security benefit [30].
- **NAS messages without protection:** Some 5G NAS messages can be sent without security protection. Examples include REGISTRATION REQUEST, AUTHENTICATION REJECT,

and REGISTRATION REJECT or SERVICE REJECT with certain causes. The study is assessing the risks of these messages for 6G, considering the impact on both the UE and the network.

- **UE AI agents:** When an UE AI agent communicates with the Core Network, the communication needs confidentiality, integrity and replay protection.

Solution Directions

- **NAS security for single and modular NAS:** With a single termination point, the 5G approach can be reused, with a 6G key set identifier and 6G algorithms in the NAS Security Mode Command procedure. With modular NAS, each NAS function needs appropriate security protection, with keys derived from common primary-authentication keying material where required by the selected architecture. Proposed approaches include separate security contexts for different Core Network functions, a dedicated routing function that terminates NAS security, and two layers of protection, one towards the routing function and one towards each network function.
- **Separate security anchor:** Several proposals derive NAS keys in a security anchor function that is kept separate from the AMF, such as a dedicated instance of that function or a Security Key Management Function (SKMF). Such an anchor could also support key separation, if the key for a new serving AMF is derived by the anchor rather than from the previous AMF's key. No dedicated solution for NAS key separation has yet been documented.
- **Operator-service signalling:** The proposals protect this signalling with keys derived from primary authentication. Over NAS, this uses a dedicated NAS security context. Over the user plane, it uses an end-to-end security context between the UE and the target network function, or a proxy acting for it.
- **Home Network security anchor:** Primary authentication can set up a reusable security context between the UE and the Home Network, with the serving network only carrying the protected information. The proposals differ in which Home Network function terminates the protection: a dedicated Home Network security function, each target Home Network function individually, or a Home Network function such as the UDM using a shared key, K_HSAF (Home Security Anchor Function key), so that it acts as both the signalling endpoint and the security endpoint.

Research and Standardisation Considerations

- Complete the security analysis once the NAS termination model is decided and align algorithm selection and key activation with the ongoing study on authenticated encryption for 6G.
- Define the MAC length values. The interim agreement is that the MAC length is fixed for each case, such as NAS, RRC and user plane over RAN; the exact values, and whether they differ between cases, are still open.
- Define the 6G key hierarchy, the placement of the security anchor and the requirements for NAS key separation.
- Decide the security endpoints for Home Network communication, whether confidentiality is needed in addition to integrity, and the format of protected parameters.
- Define the security requirements for communication between UE AI agents and Core Network functions, including the relationship to existing NAS, user-plane and any new communication-plane security.
- Define the interworking security requirements and complete the risk assessment of NAS messages sent without protection.
- Evaluate the candidate proposals and converge on a consistent solution for each function.

B. Interconnect and Roaming

When a UE roams, its communication with the Core Network also depends on signalling between the visited and home networks. In 5G, the SEPP sits at the edge of each PLMN and connects to the SEPP of another PLMN over N32. When service-based interfaces are used across PLMNs, the SEPP acts as a non-transparent proxy. TS 33.501[33] protects N32 traffic either by TLS directly between the SEPPs, or by application-layer security (PRINS, the Protocol for N32 Interconnect Security) when roaming intermediaries are on the path; up to two roaming intermediaries may be present between two SEPPs [25]. The security study covers end-to-end roaming security, including roaming intermediaries, in coordination with the GSMA. Relevant attacker locations in the study's attacker model include an attacker on the interconnect interface between operators, and an attacker in another network or a rogue network operator [30].

Security and Privacy Challenges

- **Fraud across networks:** Roaming relies on trust between operators, and a network with a valid roaming agreement can misuse that trust. The study identifies three examples: a visited network claiming inflated charges for data usage in local breakout, a network that is not serving the subscriber accessing subscription data, and a compromised or fraudulent network function invoking UDM service operations such as Nudm_SDM_Get or Nudm_UECM_Registration.
- **Home-network control:** In 5G, home control is limited to AMF registration. A visited AMF may send a registration without performing primary authentication, leaving the UDM to either trust the AMF or trigger primary authentication, which the visited network may not honour. Rejecting the request may deny service to a legitimate UE, while accepting it may give the Home Network a false location for the UE. A visited network function could also register as the serving function for a UE that is not present. A false UE location can be used for charging fraud or to steer incoming traffic to the wrong visited network.
- **Roaming intermediaries and SEPP deployments:** The study considers different roaming-intermediary and SEPP deployment models described in the 5G and GSMA specifications. Examples include an Outsourced SEPP, operated by a service provider on behalf of a PLMN, and a Group SEPP, operated as a central entity for an operator group. End-to-end protection across the interconnect needs to consider which party operates the network edge in each model, and which parties are on the path [30].
- **Trust anchors across trust domains:** A PLMN, a non-public network or a neutral host provider can each form a separate trust domain, and each may run its own Public Key Infrastructure (PKI). Its root Certificate Authority (CA) certificate then has to be distributed to other domains. Without automated life-cycle management, certificate expiry or renewal can disrupt network entities that depend on it. Without secure distribution, a false or compromised trust anchor could enable impersonation and man-in-the-middle attacks [5].

Solution Directions

- **Home control beyond registration:** One proposed approach extends home control to later procedures. The UDM validates each request, using UE mobility information from the source AMF or the subscription data, and rejects requests from networks the UE is not moving to.
- **Proof of UE presence:** Other proposed approaches give the Home Network evidence that the UE is present in the serving network, either by having the Home Network send a fresh challenge that the UE answers using keys from an earlier primary authentication, or by having the UE

add fresh evidence to existing registration, mobility or service requests. In both cases, the serving network only forwards the information and cannot modify it.

- **Limited validity for visited networks:** One proposed approach gives the visited network a temporary Subscription Permanent Identifier (SUPI) and a validity time for its security context. When the validity time expires, the corresponding security context is no longer valid for use by the visited network.

Research and Standardisation Considerations

- Select among the fraud-prevention approaches, considering which Home Network entity performs the verification, what triggers it and the signalling cost.
- Complete, with the GSMA, the description of IPX roaming hubs, IPX service hubs and Hosted SEPPs, and define what each intermediary may access or modify.
- Specify automated life-cycle management for root CA certificate distribution across trust domains.

C. Security within the Core Network

In the 5G Core Network, network functions communicate over service-based interfaces. This communication is protected at the transport layer, typically by TLS. In indirect communication, a Service Communication Proxy (SCP) is placed between network functions [24][28][29]. SA2 is studying enhancements to the Service-Based Architecture (SBA) framework for 6G [31].

Security and Privacy Challenges

Where protection terminates: In the 5G SBA security model, TLS protects communication between the communicating endpoints. In cloud deployments, TLS may instead terminate at a load balancer, gateway or sidecar before traffic reaches the network function. When TLS is terminated at the SCP, the TLS protection applies between adjacent endpoints, not across the complete path between the communicating network functions. In both cases, application data becomes available at an intermediate function outside the network function itself.

- **Security domains within the network:** Network functions of the same PLMN may belong to different security domains, for example the AMF and the SEPP. The 6G security architecture needs to define these domains, and trust anchors need to be distributed between them securely and automatically.
- **User-plane communication:** Protection of the user plane within the 6G Core Network is under study. Solutions will be considered once related transport-layer protocol work has made sufficient progress.

Solution Directions

These directions aim to keep communication protected when security terminates at gateways, sidecars, SCPs or other intermediate functions.

- **Protection of the path to the network function:** Where TLS terminates outside the network function, the path between the termination point and the network function should either lie within the same security domain or be protected separately. Where information needs protection beyond a single hop, protection at the application layer that does not depend on the transport can be considered.

- **Defined security domains:** The 6G security architecture should identify the security domains in the Core Network and the functions at their boundaries.

Research and Standardisation Considerations

- Align with SA2 work on the SBA framework.
- Study protection of Core Network communication where TLS terminates at gateways, sidecars or SCPs.
- Define the 6G security domains and the distribution of trust anchors between them.
- Study user-plane security within the Core Network as related protocol work progresses.

5. Data Collection for Security Monitoring

Collection of security-relevant information provides the security related events collection entity with data for detecting and investigating potential security incidents. 5G already defines security-related events for security monitoring through 3GPP TS 33.502[34]. The specification defines six security-related events at the SBA layer, including the conditions for detecting these events and the information to be included when they are reported.

Six security-related events are defined for collection and security monitoring, and they cover events that may indicate abnormal or unauthorized behaviour within the network:

- **Malformed messages** — messages that are invalid according to the protocol specification or network state.
- **Authorization failures** — failed authorization attempts for inbound SBA connections.
- **Authentication failures** — failed authentication attempts for inbound SBA connections.
- **Massive number of incoming messages** — repeated overload conditions caused by a large number of incoming messages.
- **SBA parameter configuration changes** — changes to SBA-level parameters, including NF certificates, NF profiles and communication-model configuration.
- **Unexpected communication-model flows** — communication flows that do not comply with the specified communication procedures or communication model.

Each event includes common information such as the event name, event code, event instance, originating network function, criticality and event timestamp, providing context about the detected event and its source.

For 6G, the existing 5G mechanism provides a starting point, while the security study considers a broader approach to security-relevant data collection across the Core Network (CN), Operations and Management (OAM), and UE-to-network communication [30]. The study also considers mechanisms for capturing and transporting this data to a security-relevant data collection entity. The specific catalogue and contents of security-relevant data remain under study.

Security and Privacy Challenges

Scope of security-relevant data: 6G's broader monitoring scope raises the question of what security-relevant information needs to be collected, and how it should be correlated across the CN, OAM and UE-to-network domains — since the existing six-event model was built specifically for the 5G SBA layer and may not give sufficient visibility beyond it. What data is relevant depends on threats and architectural mechanisms still being worked out for each domain, so the study deliberately avoids locking in a fixed data catalogue at this stage.

Protecting and isolating the monitoring channel: Security-monitoring data itself needs protection from unauthorized access or modification, since a compromised monitoring channel would undermine the reliability of any analysis built on it. The current 6G study in 3GPP has agreed to keep this traffic logically separated from user-plane and control-plane traffic to avoid interference between them — though how that separation is achieved remains unresolved and may depend on operator and regional requirements.

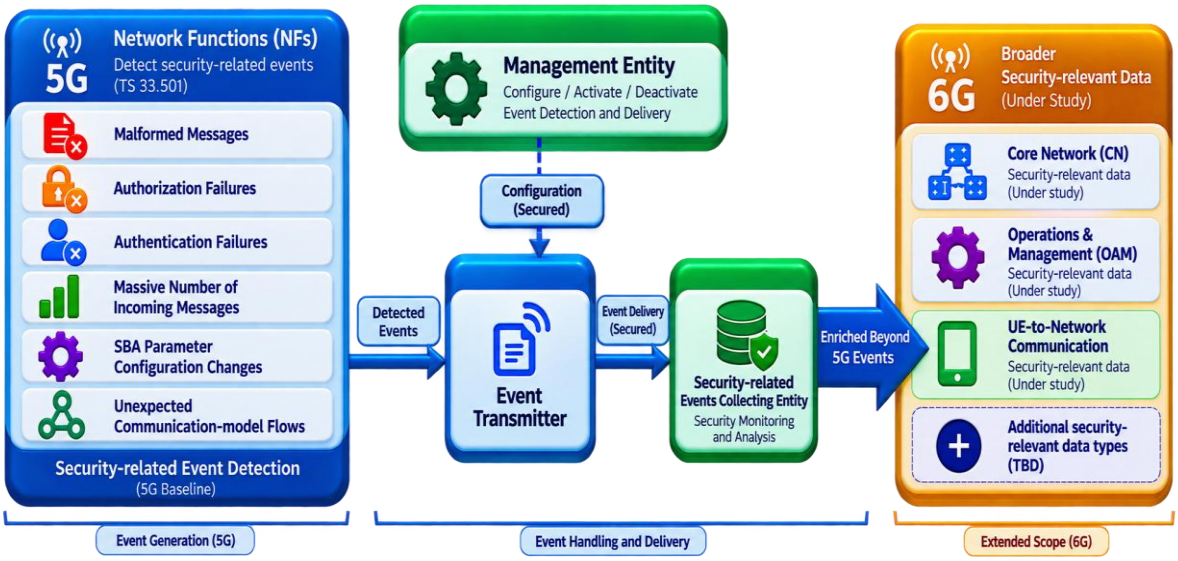

Figure 6: Security related events collection

Solution Directions

There is consensus that 6G security monitoring should build upon the event collection mechanisms established for 5G while extending visibility beyond the existing SBA event model, as illustrated in Figure 6:

- **Extend the 5G Event-Based Approach:** The six security-related events defined in TS 33.502[34] can provide a starting point for 6G security monitoring. These events can be retained while extending monitoring to additional security-relevant data from the CN, OAM and UE-to-network communication domains [30].
- **Define a Security-Relevant Data Framework:** 6G should support collection of security-relevant data beyond individual predefined events. The framework should provide sufficient context about the source, time and nature of the observed activity to support analysis and correlation across different network domains.
- **Protect and Isolate Security-Monitoring Traffic:** Security-relevant data should be protected during collection and transport using appropriate authentication, confidentiality, integrity and replay protection. Security-monitoring traffic should also be separated from user-plane and control-plane traffic to reduce interference with other network traffic.
- **Support Attack-Chain Reconstruction:** The monitoring framework should correlate observations across time and network domains to reconstruct the progression of an attack. This can help distinguish isolated anomalies from coordinated sequences of activity spanning multiple network functions, management systems and UE interactions.
- **Enable Closed-Loop Security Operations:** Security monitoring could evolve beyond detection by providing security assessments and policy-controlled response actions. Monitoring, analysis and response should operate as a continuous feedback loop, with appropriate authorization and safeguards for automated actions.

Research and Standardisation Considerations

6G security monitoring is expected to build on the security-related events already defined for 5G, but whether these need to be extended with additional data sources and mechanisms remains under study.

Further work is therefore needed to establish a common approach for identifying, collecting and protecting security-relevant data across different network domains

- **Security-Relevant Data and Event Model:** Define the scope and characteristics of security-relevant data required for continuous monitoring and assess whether the six security-related events defined in TS 33.502[34] remain sufficient for 6G or need to be complemented with additional events and data sources.
- **Cross-Domain Collection and Correlation:** Establish common approaches for collecting, transporting and correlating security-relevant data across the CN, OAM and UE-to-network communication domains, including suitable interfaces and data formats.
- **Protection and Traffic Separation:** Specify requirements for protecting security-monitoring data during collection and transport, including authenticity, integrity, confidentiality and replay protection. The approach for separating security-monitoring traffic from user-plane and control-plane traffic also requires further study.
- **Monitoring Scope and Automated Response:** Clarify the scope and interfaces of security-monitoring functions, including the treatment of RAN-related monitoring, and study the authorization and policy requirements for integrating monitoring with automated security response.
- **Event Criticality and Risk Classification:** Define a consistent approach for assigning criticality or risk levels to security-related events and observations. The classification could consider factors such as the affected network function, severity, frequency, context and correlation with other events, enabling security-monitoring functions to prioritise events and support appropriate response decisions.

AI Security

Artificial intelligence is expected to support functions such as network optimisation, automation, security monitoring, sensing and distributed intelligence in 6G. AI systems introduce security risks related to their data, models, inputs, knowledge sources and autonomous decision-making. These risks become more significant when AI systems can interact with external systems or invoke services on behalf of users or applications. General AI security therefore needs to address both the integrity of the AI system itself and the security of the interfaces through which it interacts with other entities. Figure 7 previews the AI-agent communication scenarios — UE-to-Core Network, Core Network-to-Application Function, and UE-to-UE — discussed in Part B below.

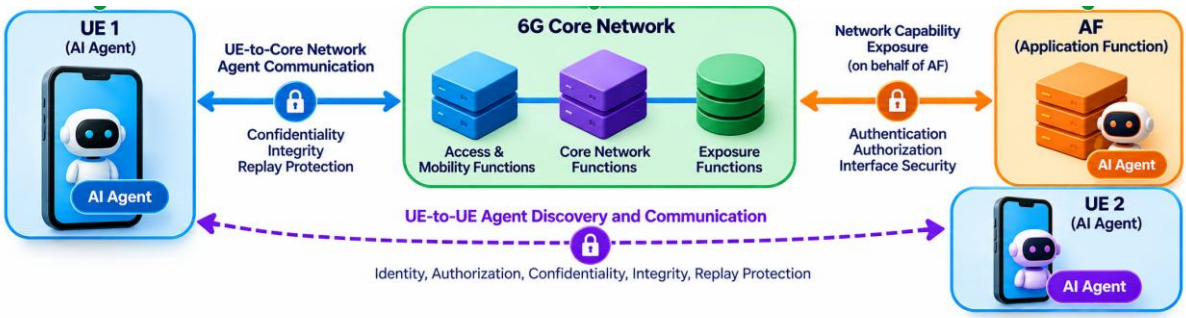

Figure 7: AI Security

This section contains two parts:

A. General AI Security
B. Security of AI Agents in 6G

A. General AI Security

AI systems bring their own set of security concerns, separate from the 6G-specific interfaces and procedures covered elsewhere in this paper [12]. These concerns span the AI system itself - its data, models and stored context, as well as the way they perform actions based on their instructions, the tools and skills they use and interaction with other agents. The list below sets out these general challenges, which apply alongside the 6G-specific considerations in Part B.

- **Data and Model Poisoning:** Manipulation of training data, fine-tuning data or AI models can influence the behaviour of an AI system and cause incorrect or malicious outputs. The integrity and provenance of data and models are therefore important throughout the AI lifecycle.
- **Adversarial Manipulation of AI:** AI systems can be affected by carefully crafted inputs designed to cause incorrect classification, prediction or decision-making. In network environments, such manipulation can affect AI-assisted monitoring, optimisation or other automated functions [10].
- **Prompt Injection and Context Manipulation:** AI systems that process natural-language or other externally supplied instructions can be influenced by malicious inputs that alter the intended context or instructions. This becomes particularly relevant when an AI system can subsequently invoke tools or network functions [20].
- **Knowledge and Retrieval Security:** AI systems may rely on external knowledge sources or retrieved information. Manipulation, unauthorized modification or injection of information into these sources can influence subsequent AI decisions and outputs.
- **Agent Goal Hijacking and Memory Manipulation:** AI agents maintain task context and may use information from previous interactions when deciding subsequent actions. Manipulation of this context or memory can cause an agent to deviate from its intended task or operate according to attacker-controlled instructions.
- **Tool Misuse and Excessive Agency:** An AI agent with access to tools or external services can potentially perform actions beyond what is required for its task if authorization boundaries are not properly enforced [21].
- **Inter-Agent Communication and Cascading Failures:** When multiple AI agents communicate or depend on each other's outputs, a compromised or manipulated agent can influence other agents [11][21].
- **AI Supply Chain Security:** AI systems depend on models, datasets, software components and supporting infrastructure obtained from different sources. Compromise of any of these components can introduce vulnerabilities or alter AI behaviour.

B. Security of AI Agents in 6G

AI agents are being studied as entities that may operate on UEs and interact with other AI agents through the 6G network. Unlike conventional AI functions, AI agents can autonomously perform tasks and interact with other entities, introducing additional security considerations. These include agent identity, registration, authorization, discovery, and communication, with different approaches under study for supporting these functions [30][31].

Security and Privacy Challenges

- **UE AI agent communication:** UE AI agents may participate in one-to-one and group communications. The security of these interactions needs to protect the exchanged information against disclosure, modification and replay. The current 6G security work specifically identifies the need for confidentiality, integrity and replay protection for communication between an UE

AI agent and the 6G Core Network, including communication associated with agent registration, discovery and subsequent interactions.

- **AI agent identity, registration and authorization:** AI agents need to be identified and associated with the authority under which they are allowed to operate. This becomes important when an agent can perform multiple tasks without continuous human intervention. Successful authentication alone should not imply unrestricted access to network functions or services: an AI agent needs to operate within the permissions associated with its authorized role and capabilities, and this authorization needs to be bound to the corresponding agent's identity so that one agent's authorization cannot be used to cover a different agent's request [21][30].
- **AI agent discovery and inter-agent communication:** The 6G architecture work considers whether and how an AI agent on one UE can discover and communicate with an AI agent on another UE through the network. This raises the same identity, authorization and communication-protection considerations as UE-to-Core Network agent communication.
- **AI agents and network capability exposure:** AI agents may also interact with network capabilities through exposure mechanisms, on behalf of an Application Function (AF) rather than as a UE's own agent — a separate strand of work from the UE AI agent topics above. Here the network needs to determine which capabilities an AI agent is permitted to invoke and under what authority. Current work on agentic exposure identifies threats including impersonation of a legitimate AF AI agent, access to network resources beyond the authorized scope, intent, role or delegated permissions, and modification, injection or observation of messages exchanged between the AI agent and the Core Network.
- **AI agent lifecycle:** An AI agent's authorization can change after it is first registered and authorized, for example when its permissions need to be extended, narrowed or withdrawn, and this needs to be reflected in later interactions rather than only at initial authorization.

Solution Directions

- For UE AI agent registration, authentication and authorization, the architecture work considers three approaches: using NAS signalling, using the user plane, or an Application Function acting on behalf of the UE. The final mechanism remains dependent on the evolving 6G architecture.
- AI agent authorization is bound to the agent's identity, so that a request can be verified as coming from the agent to which the authorization was granted.
- For UE-to-UE agent discovery and communication, the same identity-binding and authorization mechanisms developed for UE-to-Core Network agent communication apply, extended to cover agent-to-agent interactions.
- For network capability exposure to an AF's AI agent, the security work focuses on authentication, authorization and interface security for agentic communication; the specific mechanism is not yet prescribed.
- For the agent lifecycle, the 6G security study includes a requirement to support updating and revoking an UE AI agent's authorization information throughout its lifecycle.

Research and Standardisation Considerations

- Complete the UE AI agent registration and authorization mechanism once the SA2 architecture decision on NAS signalling, user plane or AF-based registration is settled, in coordination between SA2 and SA3.
- Define the security requirements for AI agent discovery and inter-agent communication as the corresponding architecture work progresses.
- Define the specific security requirements for agentic exposure to an AF's AI agent; these remain under study.
- Define the mechanism for updating and revoking UE AI agent authorization across its lifecycle, and how this is reflected in subsequent interactions.

Recommendations:

Our recommendations on 6G security are as follows:

Quantum safe 6G: 6G systems need to be safeguarded against quantum computers that threats to breaks the classical cryptography. NIST has already paved the way for post-quantum cryptography (PQC) by standardizing several quantum resistant key encapsulation mechanisms like MLKEM-512, MLKEM-768, and MLKEM-1204, and several digital signature algorithm like MLDSA-44, MLDSA-64, and MLDSA-, Several studies have also shown that these PQC algorithms do not degrade the performance of protocol compared to the case of classical algorithm. However, the PQC has not yet undergone the similar level of scrutiny as that of the classical algorithms and completely relying on them may not be safe yet. To get the benefit of established trust in the classical algorithms, and safeguard against the quantum algorithms, we recommend adopting hybrid mechanisms where both classical and PQC is used. However, these mechanisms should have the option to restrict to Post-Quantum (PQ) only mechanism to account for future scenario when there is sufficient trust in PQ-only algorithm so that 6G systems are completely safe against attacks using quantum computers.

Consent Management: New 6G features like native AI support, Sensing, computing, immersive communication, NTN is expected to generate voluminous data which could support new applications when coupled with other 6G system data related to mobility, session management, and quality of services. However, many of these data could involve user related information which when exposed without users' content can lead to privacy violations. 6G system should enforce user consent on all the exposed information to comply with the DPDP polices. As 6G is envisioned to support several AI agents, it is important that 6G system enable the operators to manage policies on how AI agents handle the users' data as per local governing laws.

SMS Security: SMS is one of the traditional services of telecommunications networks. It has evolved as one of simple and reliable means to send authentication codes (OTP) and other security related information from enterprise customers and application to end users. However, such mechanism is also allowing fraudulent activities by masking their identity. Hence, it is important that 6G network provide a mechanism to verify sender information in SMS so that that receiver has the trust on the source of the SMS origin. This is particularly relevant in India as SMS has become a default mechanism to deliver authentication codes for several services.

Security Monitoring: Malicious attack continues to evolve and apply sophisticated techniques. Detection requires collection of security-relevant events across RAN, Core Network, OAM, and UE-to-network interfaces, and correlate them to reconstruct multi-stage attacks that no single domain's view can reveal on its own. Further, 6G systems need to be proactively monitored for new discovered vulnerabilities and have the capabilities to contain any attacks that exploit these vulnerabilities or misconfigurations before causing any major damage. Thus, it is required that 6G system have the full mechanism to collect-correlate-detect-respond. Correlated findings should drive an authorized, policy-controlled response rather than alerts that stop at a human dashboard. The monitoring and response channels themselves should be logically separated from user-plane and control-plane traffic, so that a compromised monitoring path cannot itself become an attack vector.

NTN Security: 6G should incorporate NTN security from the architecture stage, ensuring that dependence on non-terrestrial infrastructure does not compromise the strategic autonomy of nations. Security should cover the service link (satellite-to-UE), feeder link (satellite-to-gateway), user terminals

and terrestrial–NTN interworking interfaces, including authentication, key management, and resilience against jamming and spoofing. The security of satellite ephemeris and timing information used for mobility and positioning should also be ensured. Secure mobility should cover transitions across satellite beams and satellites, including architectures using transparent (bent pipe) and regenerative payloads, with regenerative satellites secured as active network nodes because they process traffic onboard.

AI Agent Security: As AI agents become more capable and autonomous, 6G system should provide strong guardrails and continuous monitoring to ensure that agents operate within their authorized capabilities and intended objectives. The system should monitor agent behaviour for drift, unintended actions and deviations from authorized intent, and verify that agents correctly interpret and resolve intents before executing consequential actions. This should complement verifiable identity, authentication, authorization, secure communication, and lifecycle-based revocation.

Computing security: 6G should secure the distributed cloud, edge and network computing infrastructure that supports 6G services, with strong isolation between workloads and tenants. Security should cover workload identity and authorization, secure execution, hardware and software integrity, supply-chain assurance, and protection of sensitive data processed across distributed computing environments.

Annexure:

1. 3GPP ongoing work

The 6G work underway in 3GPP is currently being developed through three closely connected studies covering the system architecture, security, and application enablement. The architecture study, led by SA2, is defining how the 6G system itself is structured. The security study, led by SA3, is examining the security requirements and solutions associated with the evolving 6G architecture. The application-enablement study, led by SA6, is looking at how applications and application services will interact with and make use of 6G capabilities. These studies are closely interdependent: architectural choices create corresponding security questions, new ways of exposing network capabilities introduce both exposure and architectural considerations, and security requirements can in turn constrain or reshape architectural choices. In parallel, a fourth study is addressing the evolution of the 6G radio system, with coordination between the network architecture studies and the RAN work to ensure that the two evolve consistently. The results of these studies are intended to feed into Release 21, which is planned to contain the first normative 6G specifications, although not every study item needs to conclude before Release 21 work begins.

The architecture study currently spans 24 key issues covering areas such as service-based architecture, network exposure, localized services, non-3GPP access, AI within the network and through UE AI agents, integrated sensing and communication, a data framework, computing, and support for satellite and IoT access. More than one candidate architecture remains under consideration, with some elements already progressing through interim agreements. The security study addresses many of these same architectural themes through ten security areas: security architecture, RAN security, UE-to-core security, core network and interconnect/roaming security, authentication and authorization, exposure security, data collection for security monitoring, UE AI agent security, data framework security, and sensing security. These areas are further divided into specific key issues for which candidate solutions are being developed. The application-enablement study complements this work by examining how applications connect to and use the 6G system, building on concepts developed in 5G such as SEAL, CAPIF and EDGEAPP. Its scope includes capability exposure, AI/ML services and third-party AI agents, communication and computing resources, sensing, privacy across potentially untrusted domains, and digital twins. AI agents, exposure, and sensing therefore appear across all three studies, making coordination between them an important part of the ongoing work.

The Secure by Design work has also progressed from a general industry proposal into the 6G security study itself. Following the contribution “Ensuring a Secure by Design 6G System” (SP-260584), SA3 agreed to incorporate a dedicated annex on Secure by Design principles into TR 33.801-01 and to communicate these principles to other 3GPP groups through a liaison statement. The inclusion of these principles in the security study places Secure by Design directly within the ongoing technical development of 6G security, rather than treating it only as a general design objective. It also provides a basis for considering security alongside architectural decisions as the 6G system continues to evolve.

Running in parallel is the study on the 6G radio system, which addresses the evolution of the radio interface, the transition from 5G to 6G, and the organization of the future radio-access network. This work provides the radio-side foundation for Release 21 and complements the system-level architecture and security studies.

Release 21 has an approved development timeline. Package approval and the Stage-1 freeze are planned for March 2027, followed by the Stage-2 80% completion checkpoint in March 2028 and the Stage-2

freeze in June 2028. The Stage-3 freeze is planned for December 2028, followed by the ASN.1/Open API freeze in March 2029.

This makes the current study phase particularly important for 6G security. The architecture is still evolving, and decisions on exposure, AI agents, the data framework, sensing, non-3GPP access, network decomposition, and the RAN can change the relationships between system components and consequently change existing trust boundaries or introduce new ones. Security therefore needs to evolve alongside these architectural decisions. The objective of Secure by Design is to ensure that security requirements and considerations are incorporated while those decisions are being made, so that security becomes part of the resulting architecture rather than something added after the architecture has been finalized.

2. Overview of TSDSI Security Work for 6G

The evolution towards 6G is expected to integrate communication, computing, data, sensing and artificial intelligence across devices, radio networks, edge platforms, core networks and cloud environments. While these capabilities will enable new services across critical infrastructure, healthcare, transportation, manufacturing and public safety, they will also expand the security and privacy attack surface.

Security, privacy, trust and resilience should therefore be incorporated from the earliest stages of 6G design. Future networks will need to protect not only user communication, but also distributed network functions, AI models, data pipelines, sensing information, exposed network capabilities and interactions across multiple administrative domains.

Within this landscape, the Telecommunications Standards Development Society, India (TSDSI) has undertaken pre-standardisation studies covering security topics relevant to 6G and future communication systems. These activities bring together stakeholders from industry, academia and research institutions to identify threats, evaluate technology options and develop potential solution directions. Some important works are summarised below which are recently completed or ongoing.

1. Study of Post-Quantum Cryptography for Future 5G Networks and Application Verticals

The report examines the quantum threat to public-key cryptography used in telecommunications and associated application verticals. It introduces post-quantum cryptographic approaches and discusses their potential adoption in future 5G networks. The report provides an early foundation for migration planning, algorithm evaluation and quantum-resistant telecom security. [TSDSI TR 6021 V1.0.0]

2. Enhancement of the Privacy of User Subscription Identity in Future Networks

The report studies mechanisms for strengthening the privacy of permanent subscriber identities used during network access and authentication. It considers exposure and tracking risks associated with identity-protection procedures and identifies possible enhancements. The work is relevant to false base station attacks, authentication relay attacks and future subscriber-privacy mechanisms. [TSDSI TR 6032 V1.0.0]

3. Network Security Encryption Mechanism

The report examines encryption mechanisms applicable to network security and the protection of communication across network environments. It considers cryptographic protection requirements and mechanisms for maintaining confidentiality of network traffic. The study contributes to the broader evolution of secure network protocols and cryptographic architectures. [TSDSI TR 6033 V1.0.0,]

4. Security Aspects of AI/ML Models for 5G and 6G Applications

The report analyses security risks affecting AI and machine-learning models used in 5G and 6G applications. Relevant threats include data poisoning, adversarial input, model theft, malicious model modification and leakage of sensitive training or inference information. It identifies potential safeguards across the AI lifecycle, from model development and transfer to deployment and inference. [TSDSI TR 6036 V1.0.0]

5. Location Privacy-Preserving Scheme against Authentication Relay Attacks under False Base Stations

The report focuses on protecting user location privacy against authentication relay attacks involving false base stations in 5G and 6G. It studies how an attacker could relay authentication exchanges while misleading the network or user equipment about the actual access location. The proposed direction strengthens location verification while seeking to avoid unnecessary exposure of precise user-location information. [TSDSI TR 6037 V1.0.0]

6. Interoperability of Multi-Vendor QKD Hardware Using SDN

The report studies how Software-Defined Networking can coordinate Quantum Key Distribution equipment from multiple vendors. It considers common interfaces, orchestration, key management and dynamic control of QKD resources. The work supports interoperable and programmable quantum-secure networks rather than isolated, vendor-specific QKD deployments. [TSDSI TR 6046 V1.0.0,]

7. Study on Security Enablers for 6G

The report provides a broad study of security capabilities needed for trustworthy 6G networks. It considers emerging threats, evolution of cryptographic protection, lower-layer security, security architecture and protection for new 6G capabilities. The report serves as a pre-standardisation reference for identifying security gaps and potential solution directions across the 6G system. [TSDSI TR 6051 V1.0.0]

8. PQC in Embedded Systems to Secure Connected Devices

The report examines the deployment of post-quantum cryptography in embedded and connected devices. It considers the processing, memory, energy, hardware and lifecycle constraints that affect PQC implementation in resource-constrained environments. The work is particularly relevant to IoT devices, secure elements and telecom equipment that may remain deployed for long periods. [TSDSI TR 6052 V1.0.0,]

9. Multilevel End-to-End User-Plane Security Architecture for 5G, 6G and Beyond

The report studies a network-security architecture supporting multiple levels of end-to-end user-plane protection. It considers heterogeneous applications with different confidentiality, integrity and assurance requirements. The proposed direction enables application-aware security across devices, mobile networks, edge platforms and service endpoints rather than relying only on hop-by-hop network protection. [TSDSI TR 6054 V1.0.0]

10. AI/ML-Based Security Implementation in 6G Wireless Communication Systems

The report examines the use of AI and machine learning to enhance security in 6G wireless systems. It considers AI-assisted detection, analysis and response to network threats, while also recognising the need to protect the AI models, datasets and operational pipeline. The work complements model-security studies by focusing on practical AI-enabled security implementation. [TSDSI TR 6061 V1.0.0]

11. SDN-Based Optical Network for QKD: Secure and Adaptive Architecture

The report proposes a protocol-agnostic architecture integrating QKD with SDN-controlled optical networks. The framework supports monitoring of QKD link conditions, dynamic path provisioning,

coexistence of quantum and classical channels, and adaptive rerouting following failures or anomalous conditions. It also identifies needs for standard interfaces, multi-vendor interoperability, key-management integration and deployment testbeds. [TSDSI TR 6062 V1.0.0]

12. PQC Migration Strategies for 5G and 6G Mobile Networks

The report focuses on the practical transition from quantum-vulnerable cryptography to quantum-resistant mechanisms in 5G and 6G networks. It addresses migration across protocols, certificates, credentials, trust anchors and network interfaces, including coexistence of classical, hybrid and post-quantum-only mechanisms. The report supports an inventory-driven, phased migration that considers interoperability, crypto-agility and long telecom equipment lifetimes. [TSDSI TR 6064 V1.0.0]

Collectively, these reports cover identity and device trust, subscriber privacy, network encryption, AI/ML security, false base station mitigation, 6G security architecture, post-quantum migration, end-to-end user-plane protection and quantum key distribution. They demonstrate a progression from analysing individual security threats towards developing integrated, interoperable and deployment-oriented security frameworks for 6G. The ongoing WG1 portfolio also includes active work on quantum-safe lightweight sessions, authentication and key exchange for UAV and AI/ML workloads, zero-trust security for connected transportation, and further enhancement of multi-vendor QKD interoperability**.**

Acknowledgements:

This research was conducted at IIT Bombay with the contributions of the following co-authors

Name of the co-authors	organization	Email contact
Manjesh Kumar Hanawal, Prakhar Paliwal, Vinod Khandkar	IIT Bombay	mhanawal@iitb.ac.in, prakhar.paliwal@iitb.ac.in Vinodkhandkar@iitb.ac.in
Saurabh Khare	Nokia	Saurabh.khare@nokia.com
Rajavelsamy R	Samsung	rajvel@samsung.com
Sameer Kulkarni	IIT Gandhinagar	sameergk@iitgn.ac.in
Neminath Hubballi	IIT Indore	neminath@iiti.ac.in

References

1. V. -L. Nguyen, P. -C. Lin, B. -C. Cheng, R. -H. Hwang and Y. -D. Lin, "Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges," in IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2384-2428, Fourthquarter 2021, doi: 10.1109/COMST.2021.3108618.
2. P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov and M. Ylianttila, "The Roadmap to 6G Security and Privacy," in *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094-1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.
3. Ylianttila, Mika & Kantola, Raimo & Gurtov, Andrei & Muchchi, lozenzo & Opperman, Ian & Hewa, Tharaka & Liyanage, Madhusanka & Ahmad, Ijaz & Partala, Juha & Roning, Juha & Kumar, Tanesh & Ozan Özparlak, Başak & Nguyen, Tri & Lui, Fei & Abbas, Robert & Heacker, Artur & Jayousi, Sara & Martinelli, Alessio & Hass, Harald. (2020). 6G White paper: Research challenges for Trust, Security and Privacy.
4. Ericsson, 6G Security – Drivers and Needs, Ericsson White Paper, May 2024. https://www.ericsson.com/49c1cd/assets/local/reports-papers/white-papers/2024/6g-security-drivers-and-needs.pdf
5. Nokia, "Security and Trust in the 6G Era" — https://www.nokia.com/asset/210527/
6. X. Chen, W. Feng, N. Ge and Y. Zhang, "Zero Trust Architecture for 6G Security," in IEEE Network, vol. 38, no. 4, pp. 224-232, July 2024, doi: 10.1109/MNET.2023.3326356.
7. J. Groen et al., "Implementing and Evaluating Security in O-RAN: Interfaces, Intelligence, and Platforms," in IEEE Network, vol. 39, no. 1, pp. 227-234, Jan. 2025, doi: 10.1109/MNET.2024.3434419.
8. M. Polese, L. Bonati, S. D'Oro, S. Basagni and T. Melodia, "Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges," in IEEE Communications Surveys & Tutorials, vol. 25, no. 2, pp. 1376-1411, Secondquarter 2023, doi: 10.1109/COMST.2023.3239220.
9. H. Moudoud, Z. A. E. Houda and B. Brik, "Zero Trust Security Architecture for 6G Open Radio Access Networks (ORAN)," in *IEEE Networking Letters*, vol. 6, no. 4, pp. 272-275, Dec. 2024, doi: 10.1109/LNET.2024.3514357
10. Van-Tam Hoang, Yared Abera Ergu, Van-Linh Nguyen, Rong-Guey Chang, Security risks and countermeasures of adversarial attacks on AI-driven applications in 6G networks: A survey, Journal of Network and Computer Applications, Volume 232, 2024, 104031, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2024.104031.
11. S. Chatzimiltis, M. B. Mashhadi, M. Shojafar, M. Debbah and R. Tafazolli, "Agentic AI for 6G: A New Paradigm for Autonomous RAN Security Compliance," in IEEE Communications Standards Magazine, doi: 10.1109/MCOMSTD.2026.3681685.
12. NIST, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)" - https://doi.org/10.6028/NIST.AI.100-1
13. P. Dass, S. Ujjwal, J. Novotny, Y. Zolotavkin, Z. Laaroussi, and S. Köpsell, "Addressing privacy concerns in joint communication and sensing for 6G networks: Challenges and prospects," arXiv preprint arXiv:2405.01742, 2024.
14. Qu, Y., Zhang, Y., Wang, Y. et al. Secure and privacy-preserving issues in integrated sensing and communication-enabled wireless networks: a survey. EURASIP J. Adv. Signal Process. 2026, 4 (2026). https://doi.org/10.1186/s13634-025-01277-w
15. N. Su et al., "Integrating Sensing and Communications in 6G? Not Until It Is Secure to Do So," in IEEE Wireless Communications, doi: 10.1109/MWC.2026.3703015.
16. P. Porambage et al., "Security, Privacy, and Resilience Controls for the 6G End-to-End System Developed in Hexa-X-II," 2025 Joint European Conference on Networks and Communications

& 6G Summit (EuCNC/6G Summit), Poznan, Poland, 2025, pp. 727-732, doi: 10.1109/EuCNC/6GSummit63408.2025.11036931.
17. R. Zhou, H. Guo, F. E. C. Teo and S. Bakiras, "A Survey on Post-Quantum Cryptography for 5G/6G Communications," 2023 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Singapore, 2023, pp. 1-6, doi: 10.1109/SOLI60636.2023.10425346.
18. A. Hitayezu, J.-T. Wang, and T. C. Chia, “From 2G to 6G: A comprehensive survey on the evolution and enhancement of AKA protocols for next-generation wireless networks,” ICT Express, vol. 12, no. 3, pp. 630–640, 2026, doi: 10.1016/j.icte.2026.03.011.
19. M. Yang, Y. Qu, T. Ranbaduge, C. Thapa, N. H. Sultan, M. Ding, H. Suzuki, W. Ni, S. Abuadbba, D. Smith, P. Tyler, J. Pieprzyk, T. Rakotoarivelo, X. Guan, and S. Mrabet, “From 5G to 6G: A Survey on Security, Privacy, and Standardization Pathways,” ACM Computing Surveys, vol. 58, no. 8, Art. no. 193, 2026, doi: 10.1145/3785467.
20. Y. Liu, Y. Jia, R. Geng, J. Jia, and N. Z. Gong, “Formalizing and Benchmarking Prompt Injection Attacks and Defenses,” in Proc. 33rd USENIX Security Symposium (USENIX Security 24), Philadelphia, PA, USA, 2024, pp. 1831–1847.
21. Ferrag, M. A., Tihanyi, N., Hamouda, D., Maglaras, L., Lakas, A., & Debbah, M. (2026). “From prompt injections to protocol exploits: Threats in LLM-powered AI agents workflows”. ICT Express, 12(2), 353–383. https://doi.org/10.1016/j.icte.2025.12.001
22. Ludant, N., Vomvas, M., Dimou, S., & Noubir, G. (2025). Low-layer attacks against 4G/5G networks. In Proceedings of the 18th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2025) (pp. 248–255). Association for Computing Machinery. https://doi.org/10.1145/3734477.3734725
23. Cao, J., Yang, Y., Ma, R., Li, S., & Li, H. (2025). The security overview and analysis of 3GPP 5G MAC CE [Preprint]. arXiv. https://arxiv.org/abs/2506.09502
24. R. Patil, Z. Tian, M. Gurusamy, and J. McCloud, “5G core network control plane: Network security challenges and solution requirements,” Computer Communications, vol. 229, Art. no. 107982, 2025, doi: 10.1016/j.comcom.2024.107982.
25. O. Zeidler, D. Fraunholz, J. Sturm, H. König and W. Kellerer, "Performance Evaluation of 5G Roaming Security Based on PRINS," 2025 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 2025, pp. 1-10, doi: 10.1109/CNS66487.2025.11195047.
26. N. Wehbe, H. A. Alameddine, M. Pourzandi, and C. Assi, “Empowering 5G SBA security: Time series transformer for HTTP/2 anomaly detection,” Computers & Security, vol. 148, p. 104114, 2025, doi: 10.1016/j.cose.2024.104114.
27. Aiello, S.T.; Rimal, B.P.; Sheldon, F.T.; Wang, Y. Investigating Security Vulnerabilities in 5G Control and User Planes: Attack Patterns and Protection Strategies. J. Cybersecur. Priv. 2026, 6, 37. https://doi.org/10.3390/jcp6010037
28. A. Atutxa, J. Astorga, A. Sanz, and E. Jacob, “Secure the Core: A novel approach for secure and efficient communication in Service-Based Architectures and beyond 5G networks,” Journal of Network and Computer Applications, vol. 250, p. 104481, 2026, doi: 10.1016/j.jnca.2026.104481.
29. O. Zeidler, J. Sturm, D. Fraunholz, and W. Kellerer, “Performance Evaluation of Transport Layer Security in the 5G Core Control Plane,” in Proc. 17th ACM Conf. Security and Privacy in Wireless and Mobile Networks (WiSec ’24), Seoul, Republic of Korea, 2024, pp. 78–88, doi: 10.1145/3643833.3656140.
30. 3GPP TR 33.801-01, "Study on Security for the 6G System," V0.6.0, 3GPP, Sep. 2026.
31. 3GPP TR 23.801-01, "Study on Architecture for 6G System; Stage 2," V0.9.0, 3GPP, Sep. 2026.
32. 3GPP TR 23.801-02, "Study on 6G Application Enablement," V0.4.1, 3GPP, Sep. 2026.
33. 3GPP TS 33.501, "Security Architecture and Procedures for 5G System," V20.3.0, 3GPP.
34. 3GPP TS 33.502, "Security-related Events Handling," V20.1.0, 3GPP, Jun. 2026. Available:

35. 3GPP TS 33.203, "3G Security; Access Security for IP-based Services," V20.0.0, 3GPP, Jun. 2026.
36. 3GPP TS 23.228, "IP Multimedia Subsystem (IMS); Stage 2," V20.1.0, 3GPP, Sep. 2026.
37. 3GPP TS 23.040, "Technical Realization of the Short Message Service (SMS)," V20.0.0, 3GPP, Sep. 2026.
38. 3GPP TR 38.901, "Study on Channel Model for Frequencies from 0.5 to 100 GHz," V19.5.0, 3GPP, Sep. 2026.

Bharat6G Alliance

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

info@bharat6galliance.com

www.bharat6galliance.com