6G SNS IA

Smart Networks and Services Industry Assocation

Security Working Group

Innovative Approaches for 6G Security

Challenges, Solutions, and Impact

POSITION PAPER

January 2025

DOI: 10.5281/zenodo.14619618
URL: https://doi.org/10.5281/zenodo.14619618

Co-funded by the European Union

smart-networks.europa.eu

Executive Summary

This paper addresses cutting-edge research and innovative solutions in the realm of 6G security, emphasizing the importance of trustworthiness, privacy, and resilience in future network architectures. Looking at collaborative projects funded by EU through SNS JU calls, it provides a comprehensive overview of 6G security research challenges in scope ranging from distributed cloud systems to physical layer protection.

This paper is organized around the following key pillars depicting research clusters covered by projects:

1. Innovative Security Frameworks:
    - Projects like DESIRE-6G and iTrust6G propose AI-driven architectures for dynamic and continuous trust evaluation (zero-trust) and adaptive security orchestration.
    - SAFE-6G introduces a holistic trustworthiness framework addressing safety, security, privacy, resilience, and reliability as integral elements.
2. Decentralized and Adaptive Solutions:
    - The RIGOROUS project leverages decentralized resource management and security architectures to enable seamless integration across the Cloud-Edge-IoT continuum.
    - PRIVATEER emphasizes privacy-first security through decentralized analytics, secure orchestration, and proof-of-transit mechanisms.
3. Advanced Technologies for Future-Ready Networks:
    - NATWORK focuses on AI-enhanced physical layer security to combat jamming and eavesdropping threats, optimizing MIMO and RIS strategies.
    - Hexa-X-II develops SPR (Security, Privacy, Resilience) controls for 6G, including post-quantum cryptography and federated learning for anomaly detection.
4. Scalable and Zero-Touch Approaches:
    - ACROSS introduces an automated, zero-touch provisioning framework for cross-domain services with robust remote attestation mechanisms and Network Digital Twins (NDTs) for realistic dataset generation, AI model validation, and service optimization.
    - 6G-BRICKS integrates Software-Defined Perimeters and Zero Trust Architectures for adaptable and efficient security management.

Each project identifies gaps in the current B5G and 6G security landscape and provides targeted solutions for challenges like cross-domain trust, dynamic service topology, and the lack of holistic, continuous trust evaluation. Collectively, these initiatives form the foundation for a secure, user-centric, and resilient 6G ecosystem capable of addressing future cybersecurity threats.

Contents

1 ABBREVIATIONS

6G	Sixth Generation (mobile networks)
AAA	Authentication, Authorization, and Accounting
AI	Artificial Intelligence
AIMLF	AI/Machine Learning Framework
DLT	Distributed Ledger Technology
D-MUTRA	DLT-Mutual Remote Attestation
E2E	End-to-End
GDPR	General Data Protection Regulation
IDAN	Intent-Driven Autonomous Networks
IoC	Indicators of Compromise
IoT	Internet of Things
KPI	Key Performance Indicator
LoT	Level of Trust
ML	Machine Learning
MLFO	Machine Learning Function Optimizer
MIMO	Multiple-Input, Multiple-Output
NWDAF	Network Data Analytics Function
PQC	Post-Quantum Cryptography
PLD	Physical Layer Deception
PKG	Physical Layer Key Generation
QoS	Quality of Service
RAN	Radio Access Network
RIS	Reconfigurable Intelligent Surface
SBA	Service-Based Architecture
SECaaS	Security as a Service
SDS	Software-Defined Security
SDN	Software-Defined Networking
SDP	Software-Defined Perimeters
SLA	Service Level Agreement
SMO	Service Management and Orchestration
SON	Self-Organising Networks
SoTA	State of the Art
TDD	Time Division Duplexing
TMF	Telemanagement Forum
TOSCA	Topology and Orchestration Specification for Cloud Applications
TPM	Trusted Platform Module
UE	User Equipment
VM	Virtual Machine
ZT	Zero Trust
ZSM	Zero-Touch Service Management

2 INTRODUCTION

As the transition to 6G networks accelerates, the landscape of security, privacy, and trust challenges grows increasingly complex. This document serves as a comprehensive paper, outlining the critical challenges and corresponding solutions required to ensure the robustness of future network architectures. It highlights the limitations of current 5G systems and proposes innovative approaches tailored for the dynamic, heterogeneous, and distributed environments of 6G.

The following sections delve into the most pressing challenges and their potential solutions, encompassing areas such as decentralized security frameworks, privacy-preserving technologies, adaptive trust mechanisms, and quantum-resilient cryptographic systems. Additionally, the document explores use cases, research priorities, and strategic recommendations that are vital for shaping secure and trustworthy 6G ecosystems. This structured approach provides a roadmap for stakeholders, researchers, and policymakers to navigate the complexities of next-generation networks effectively.

3 Innovative Security Frameworks

The evolution toward 6G necessitates transformative approaches to ensure robust, secure, and trustworthy networks. The DESIRE-6G, iTrust6G, and SAFE-6G projects address this challenge with groundbreaking solutions tailored to the unique demands of next-generation networks. Their collective research introduces foundational advancements in security frameworks that integrate trustworthiness as a core tenet.

3.1 Research statement and perspective

DESIRE-6G pioneers a blockchain-enabled mutual remote attestation framework to ensure software agent trustworthiness. By integrating Distributed Ledger Technology (DLT) with AI-driven Multi-Agent Systems (MAS), this approach allows dynamic and platform-agnostic security verification. Agents, autonomously instantiated by Machine Learning Function Optimizers (MLFOs), perform remote attestations before execution, ensuring their integrity within heterogeneous environments.

Key innovations include:

- A DLT-Mutual Remote Attestation (D-MUTRA) mechanism providing zero-touch, sustainable, and continuous security verification.
- Elimination of infrastructure constraints, enabling deployment across diverse domains (e.g., RAN, edge, cloud).

- Auditable and immutable attestation records via blockchain, enhancing transparency and scalability.

These advancements address critical gaps in existing attestation frameworks by eliminating dependencies on hardware-specific solutions and enabling distributed verification mechanisms. This ensures seamless and secure service deployment in dynamic 6G ecosystems.

The iTrust6G project [6] introduces a comprehensive security and trust orchestration architecture to adapt to the dynamic and distributed nature of 6G environments. By leveraging AI, iTrust6G creates a trust and security management framework instrumenting Zero-Trust paradigm [10]. One key pillar is a continuous trust evaluation of assets involved in networks, integrating:

- Remote attestation for runtime integrity checks.
- Supply chain vulnerability analysis.
- Behavioral analysis for real-time trust adaptation.

This architecture combines federated learning and generative AI to enhance threat detection, classification, and mitigation. Its dynamic trust evaluation framework delivers a comprehensive trust score derived from both static and dynamic analyses, enabling precise and informed security decisions. The supervision of programmable security controls located close or in-situ of network functions ensures adaptability across diverse scenarios while reducing security overheads.

Key contributions include:

- AI-enhanced security orchestration, leveraging federated learning and generative AI.
- Modular trust frameworks supporting various standards and architectures.
- Dynamic service topology adaptation, enabling continuous and holistic trust assessments.

SAFE-6G addresses the need for a holistic trustworthiness paradigm, integrating safety, security, privacy, resilience, and reliability as dimensions of a user-centric 6G system. The project underscores the transition from traditional security models to a broader trustworthiness framework, balancing usability and agility with robust security-by-design principles.

Highlights of SAFE-6G's research include:

- AI-driven cognitive coordination components for intent-based trustworthiness management.

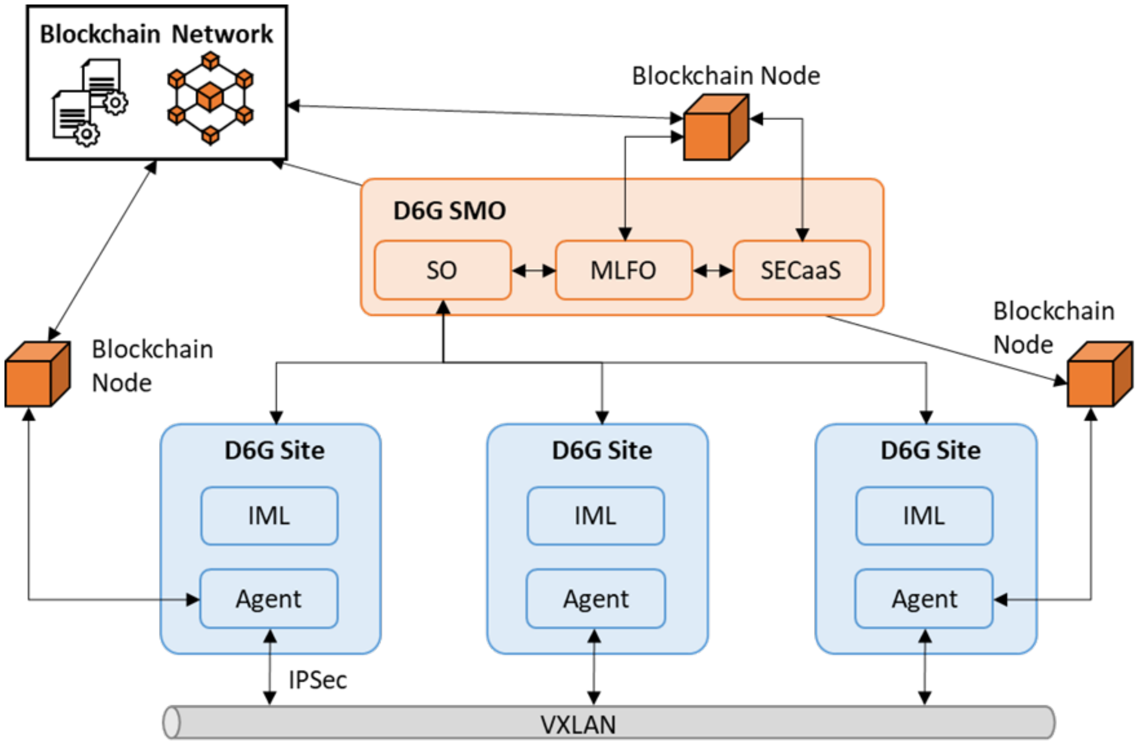


Figure 1: General representation of three distributed agents over several domains, ready for remote attestation through the SECaaS.

- A clear distinction between trust (user perception) and trustworthiness (system property), fostering transparent and adaptive security mechanisms.
- Integration of novel cognitive and AI/ML techniques to align trustworthiness with user-centric requirements.

This paradigm shift enables 6G systems to dynamically adapt trustworthiness levels to the specific needs of tenants and users, ensuring security and reliability across heterogeneous and distributed environments.

3.2 Architecture Innovations and Solutions

DESIRE-6G introduces an architecture depicted in Fig. 1 that focuses on AI-powered Multi-Agent Systems (MAS) and platform-agnostic remote attestation. The MAS are dynamically configured by Machine Learning Function Optimizers, optimizing resource management and improving coverage efficiency across various domains. To ensure integrity and trustworthiness, the system employs a blockchain-enabled attestation mechanism. This approach eliminates traditional dependencies, allowing software components to independently measure and verify their integrity while maintaining high levels of security and operational efficiency.

The integration of distributed verifier capabilities and the use of blockchain principles align with the decentralized nature of 6G networks. By incorporat-

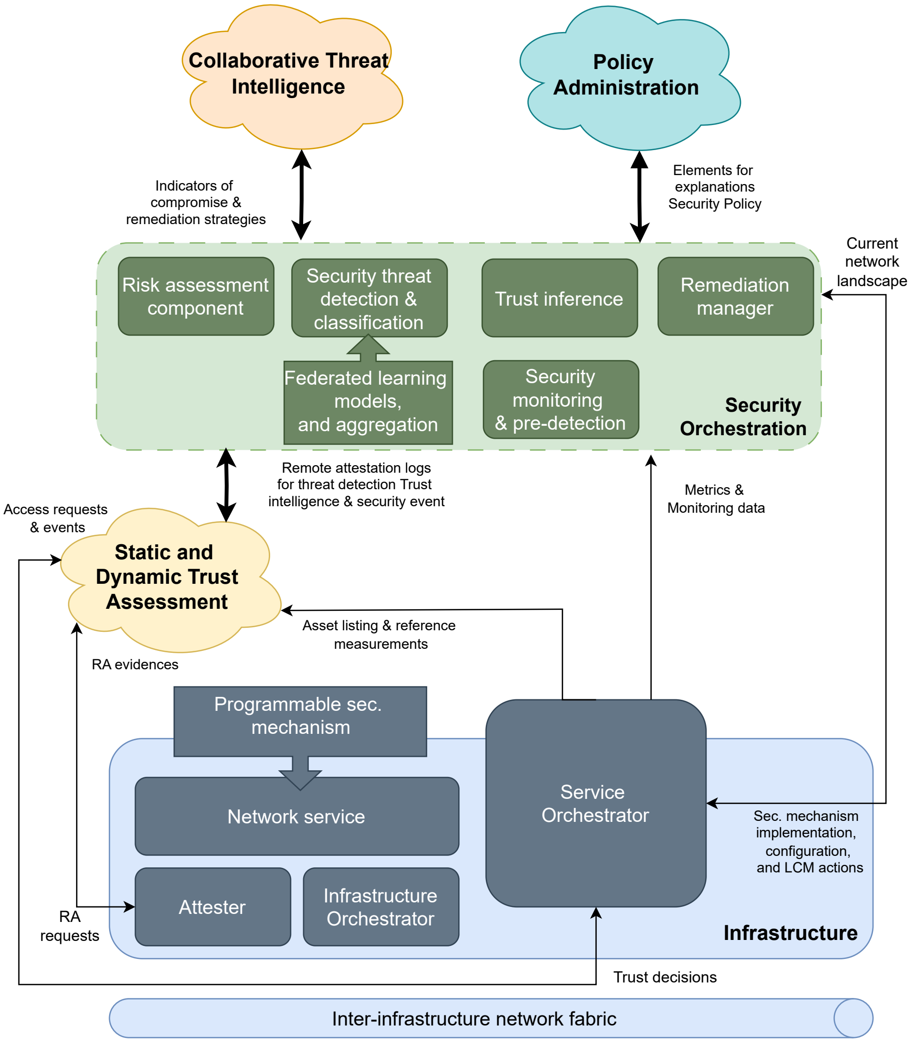

Collaborative Threat Intelligence
Policy Administration
Indicators of compromise & remediation strategies
Elements for explanations Security Policy
Current network landscape
Risk assessment component
Security threat detection & classification
Trust inference
Remediation manager
Federated learning models, and aggregation
Security monitoring & pre-detection
Security Orchestration
Remote attestation logs for threat detection Trust intelligence & security event
Metrics & Monitoring data
Access requests & events
Static and Dynamic Trust Assessment
Asset listing & reference measurements
RA evidences
Programmable sec. mechanism
Network service
Service Orchestrator
Sec. mechanism implementation, configuration, and LCM actions
Attester
Infrastructure Orchestrator
RA requests
Infrastructure
Trust decisions
Inter-infrastructure network fabric

Figure 2: iTrust6G Security Orchestrator and Infrastructure Architecture

ing continuous integrity verification methods, the architecture minimizes performance penalties, ensuring seamless operation even under stringent security requirements.

iTrust6G's architecture is built around an AI-driven security orchestrator and a comprehensive trust evaluation framework. The security orchestrator, presented in Fig. 2 employs federated learning and generative AI to detect threats, classify vulnerabilities, and automate remediation strategies. Complementing this, the trust evaluation framework integrates behavioral analysis, supply chain vulnerability assessments, and real-time attestation processes to provide dynamic and accurate trust scores, as illustrated in Fig. 3. This trust score will impact the access given to resources accessing the network and the security supervision of the domains.

The architecture's modular design facilitates adaptability across diverse environments, supporting scalable implementations and enabling precise security

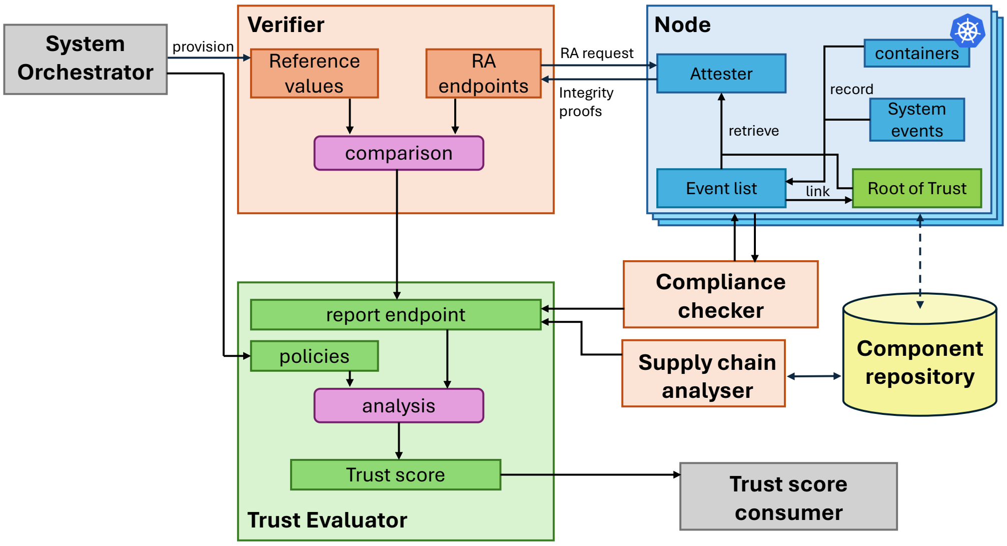


Figure 3: Representation the iTrust6G trust evaluation over an entity, including all actors involved

controls. By providing programmable interfaces to security mechanisms and relevant virtualisation model [3], the system ensures that network services can be monitored and protected in real-time while serving posture analysis for trust assessment, making it a robust solution for dynamic 6G landscapes.

SAFE-6G presents a user-centric architectural framework that integrates AI-driven cognitive coordination to dynamically manage trustworthiness. This system interprets user-defined intents and translates them into actionable configurations across multiple dimensions, including safety, security, privacy, resilience, and reliability. The framework's adaptability allows it to align trustworthiness levels with specific user or tenant requirements, ensuring a tailored and efficient security posture.

By leveraging advanced AI and machine learning techniques, SAFE-6G bridges the gap between user expectations and system operations. This coordination ensures that the architecture remains flexible and responsive, meeting the evolving demands of 6G networks while maintaining robust security and usability.

3.3 Impact on 6G and filled security gaps

DESIRE-6G addresses the critical need for securing complex services in heterogeneous environments by providing continuous, platform-independent attestation mechanisms. This approach ensures that services can be configured and executed without performance degradation or reliance on pre-installed infrastructure security measures. By enabling decentralized verification through distributed agents, DESIRE-6G fosters a scalable and adaptable security model that

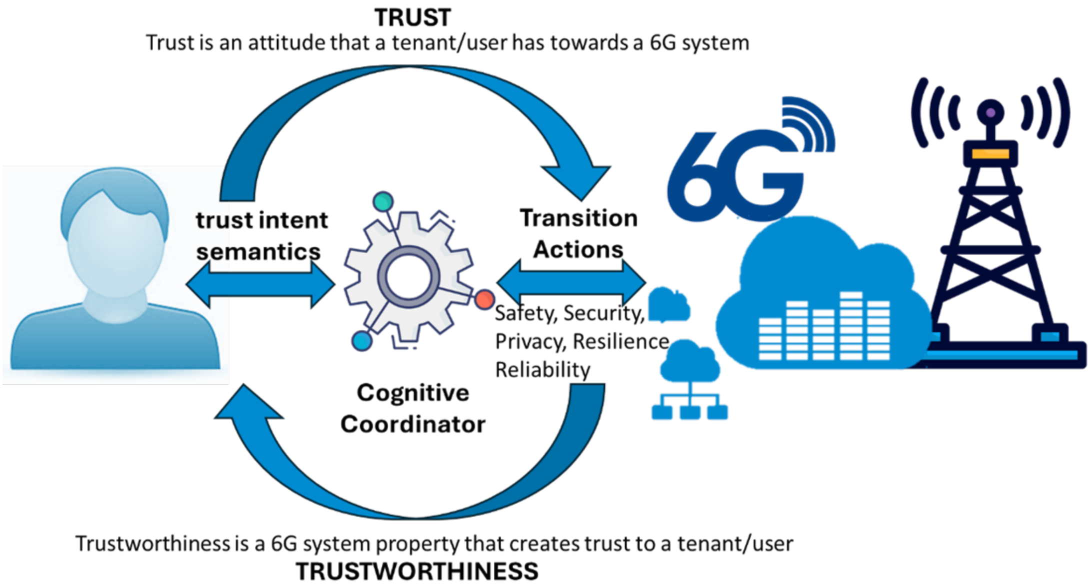

TRUST
Trust is an attitude that a tenant/user has towards a 6G system
trust intent semantics
Transition Actions
Safety, Security, Privacy, Resilience Reliability
Cognitive Coordinator
6G
Trustworthiness is a 6G system property that creates trust to a tenant/user
TRUSTWORTHINESS

Figure 4: User-centric and AI-assisted coordination of 6G trustworthiness

aligns with the dynamic nature of 6G networks. The emphasis on sustainable integrity verification during runtime enhances trust in service deployment and operation, filling gaps in existing security frameworks.

iTrust6G tackles the limitations of static and reactive security systems by introducing a dynamic, AI-driven approach that integrates trust evaluation into every layer of the network. The project's federated learning models enhance scalability compared to the current state-of-the-art (e.g. [9, 2]), allowing distributed systems to process vast amounts of data without overwhelming centralized resources. Additionally, the use of adaptive playbooks ensures proactive responses to emerging threats, addressing vulnerabilities before they compromise network integrity, as it is generally the case nowaday [7]. By focusing on cross-domain collaboration and trust architectures, iTrust6G provides a comprehensive framework for real-time threat management and trust maintenance, bridging gaps in current cybersecurity practices.

SAFE-6G's impact lies in its holistic approach to trustworthiness, encompassing safety, security, privacy, resilience, and reliability. The project's user-centric design enables networks to dynamically adapt to individual trust requirements, ensuring tailored security measures for diverse stakeholders. By integrating cognitive AI for intent-based trust management, SAFE-6G delivers an unprecedented level of adaptability and transparency. This paradigm shift from security-only frameworks to a broader trustworthiness model addresses the evolving demands of 6G ecosystems, filling critical gaps in usability, agility, and reliability.

3.4 Recommendations for Advancing 6G Security Frameworks

Building on the contributions of DESIRE-6G, iTrust6G, and SAFE-6G, the path forward for 6G security frameworks involves embracing comprehensive, adaptive, and user-centric solutions. Key recommendations include the adoption of decentralized verification mechanisms to ensure scalability and flexibility in dynamic environments. Integrating AI-driven orchestration and trust evaluation can enhance real-time threat management and proactive response capabilities, while blockchain technology offers immutable and transparent security validation processes.

Future architectures must prioritize holistic trustworthiness, addressing dimensions such as safety, security, privacy, resilience, and reliability. Cognitive coordination mechanisms should be expanded to align system capabilities with user-defined intents, ensuring that 6G networks remain responsive and adaptable to diverse requirements. Lastly, fostering cross-domain collaboration and aligning with emerging standards will be essential to creating resilient ecosystems capable of addressing the complex challenges of next-generation networks. By uniting advanced technologies and user-centric principles, these frameworks will enable 6G networks to achieve unmatched levels of security, reliability, and trustworthiness.

4 Decentralized and Adaptive Solutions

The challenges posed by the dynamic and heterogeneous environments of 6G necessitate decentralized and adaptive solutions that prioritize security, privacy, and trust across the Cloud-Edge-IoT continuum. Projects like RIGOROUS and PRIVATEER propose groundbreaking approaches to address these challenges by fostering seamless integration, robust trust mechanisms, and privacy-first architectures.

4.1 Research statement and perspective

The RIGOROUS project, whose architecture is shown in Fig. 5, addresses the challenge of enabling trustworthy, secure, and efficient resource management in 6G networks. Its vision is focused on orchestrating decentralized security frameworks across the Cloud-Edge-IoT continuum, ensuring scalability and adaptability in heterogeneous and multi-operator environments.

RIGOROUS introduces several innovative mechanisms to achieve its goals:

- AI-Driven Security Orchestration: Dynamically enforces security policies across IoT, RAN, edge, and cloud domains, leveraging Federated Learning (FL) for seamless reconfiguration while preserving data privacy.
- Intent-Based Security Management (ISM): Translates high-level security goals into actionable configurations, resolving conflicts and ensuring consistent policy application.

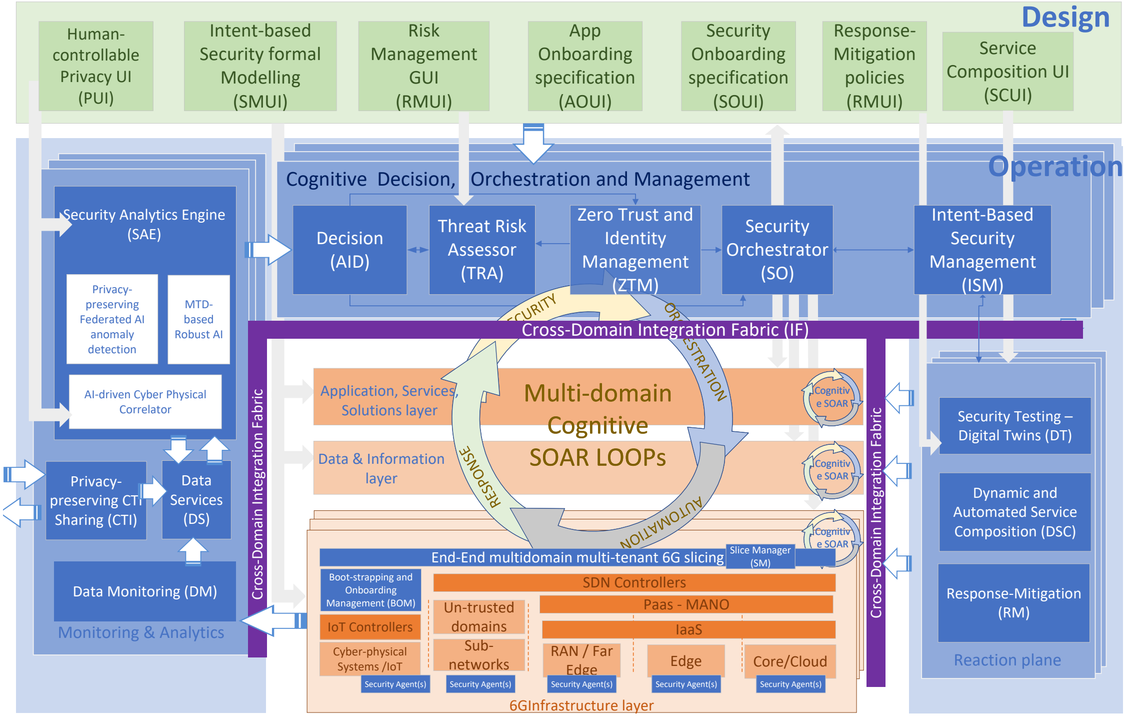

Design
Human-controllable Privacy UI (PUI)
Intent-based Security formal Modelling (SMUI)
Risk Management GUI (RMUI)
App Onboarding specification (AOUI)
Security Onboarding specification (SOUI)
Response-Mitigation policies (RMUI)
Service Composition UI (SCUI)
Operation
Cognitive Decision, Orchestration and Management
Decision (AID)
Threat Risk Assessor (TRA)
Zero Trust and Identity Management (ZTM)
Security Orchestrator (SO)
Intent-Based Security Management (ISM)
Security Analytics Engine (SAE)
Privacy-preserving Federated AI anomaly detection
MTD-based Robust AI
AI-driven Cyber Physical Correlator
Privacy-preserving CTI Sharing (CTI)
Data Services (DS)
Data Monitoring (DM)
Monitoring & Analytics
Cross-Domain Integration Fabric (IF)
Cross-Domain Integration Fabric
SECURITY
ORCHESTRATION
AUTOMATION
RESPONSE
Multi-domain Cognitive SOAR LOOPs
Application, Services, Solutions layer
Data & Information layer
Cognitive SOAR
End-End multidomain multi-tenant 6G slicing
Slice Manager (SM)
Boot-strapping and Onboarding Management (BOM)
IoT Controllers
Cyber-physical Systems /IoT
SDN Controllers
Un-trusted domains
Sub-networks
Paas - MANO
IaaS
RAN / Far Edge
Edge
Core/Cloud
Security Agent(s)
6GInfrastructure layer
Security Testing – Digital Twins (DT)
Dynamic and Automated Service Composition (DSC)
Response-Mitigation (RM)
Reaction plane

Figure 5: RIGOUROUS High-level Functional Block Architecture (HLFA).

- Zero-Trust Management (ZTM): Implements granular access controls with real-time event analysis to detect anomalies and enable proactive threat mitigation.
- Dynamic and Automatic Service Composition (DSC): Ensures protocol compatibility and communication consistency among distributed components, enabling seamless integration in heterogeneous systems.
- Digital Twins (DT): Facilitates predictive threat detection and dynamic service reconfiguration, enhancing resilience against evolving cyber threats.
- AI-Driven Decision Engine (AID) and Threat Risk Assessor (TRA): Analyze threat contexts and prioritize mitigation strategies for precise and timely interventions.
- Privacy-Preserving Cyber Threat Intelligence (CTI) Sharing: Secures sensitive data exchanges across domains using advanced Privacy-Enhancing Technologies (PETs).
- Network Flow and Topology Monitoring: Provides continuous assessment and adaptive management of network flows, devices, and services.
- DevSecOps Alignment: Supports secure and scalable service design, deployment, and management across distributed networks.

PRIVATEER introduces a privacy-first framework tailored for 6G (shown in Fig. 6), ensuring that security mechanisms safeguard privacy without compromising functionality. The project emphasizes decentralized security analytics, privacy-aware

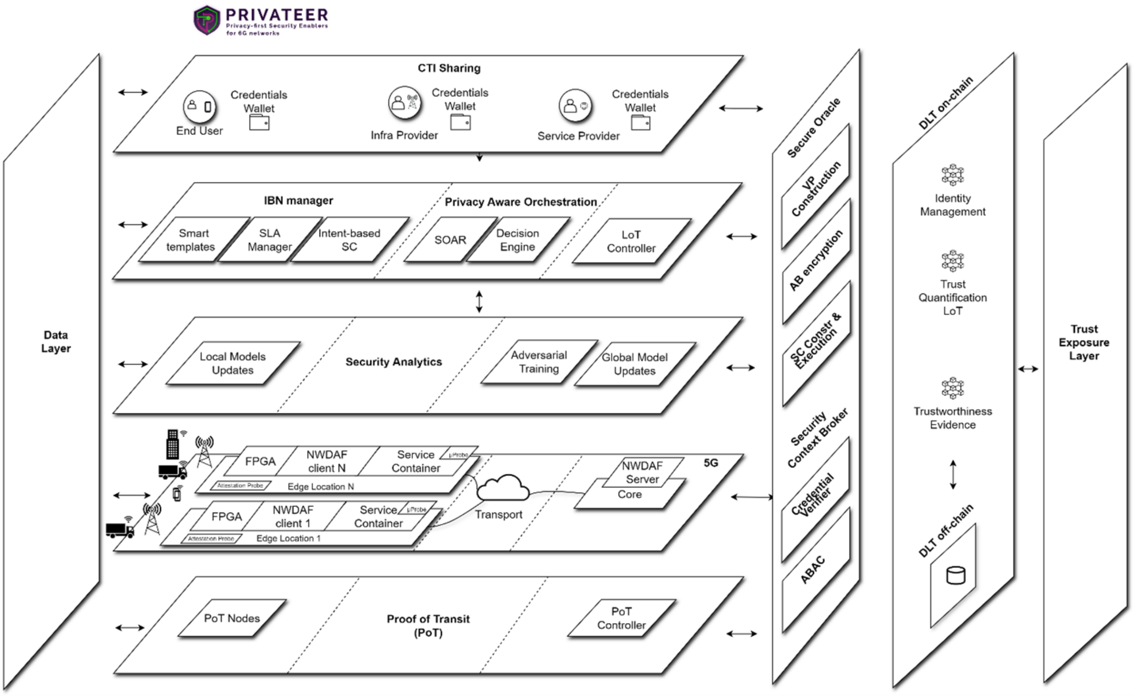


Figure 6: The PRIVATEER "Privacy-first" security architecture for 6G.

orchestration, and proof-of-transit mechanisms to maintain trustworthiness in heterogeneous networks. By leveraging federated learning and privacy-preserving data sharing, PRIVATEER enables stakeholders to collaborate on threat intelligence without exposing sensitive information.

Highlights of research include:

- Privacy-friendly Cyber Threat Intelligence (CTI) sharing using federated learning and homomorphic encryption.
- Security Orchestration, Automation, and Response (SOAR) component for lifecycle security management.
- Level of Trust (LoT) Controller evaluating end-to-end trustworthiness based on integrity, confidentiality, and resilience.
- Decentralized security analytics employing AI/ML models for anomaly detection and intrusion prevention.
- Edge-based AI/ML deployment for enhanced responsiveness and data privacy preservation.

4.2 Architecture Innovations and Solutions

RIGOROUS and PRIVATEER provide complementary advancements in architecture to support decentralized and adaptive solutions for 6G.

The RIGOROUS project delivers an advanced architecture designed to address the complexity and heterogeneity of 6G networks. A central feature is its sophisticated orchestration framework, which combines decentralized management, dynamic security enforcement, and predictive adaptability to ensure scalability and trustworthiness across the Cloud-Edge-IoT continuum.

At the core of this architecture is the AI-Driven Security Orchestrator (SO), which dynamically enforces security policies and facilitates seamless orchestration across IoT, RAN, edge, and cloud segments. This orchestrator leverages Federated Learning (FL) to deploy and adapt policies without exposing sensitive data, ensuring real-time reconfiguration while preserving privacy. The SO integrates with the Intent-Based Security Management (ISM) framework to translate high-level security goals into actionable configurations, resolving conflicts and maintaining policy consistency across domains.

The Multi-Cluster Resource Manager (MCRM) further enhances the orchestration capabilities by securing and optimizing resource allocation across distributed clusters. This component dynamically manages resource placement and migration, ensuring robust system performance even in highly heterogeneous environments. Additionally, the Dynamic and Automatic Service Composition (DSC) module supports the orchestration of services by resolving protocol mismatches and communication inconsistencies, enabling seamless integration and service functionality.

To bolster resilience, RIGOROUS incorporates an Integration Fabric that facilitates real-time threat detection and adaptive response. This fabric ensures seamless communication among architectural components, supporting the orchestrator in dynamically reconfiguring services to mitigate emerging threats. The architecture also leverages Digital Twins (DT) for predictive risk assessment and service optimization, enabling preemptive action against potential vulnerabilities.

Privacy and security are further strengthened through the Privacy-Preserving Cyber Threat Intelligence (CTI) sharing framework, which secures sensitive data exchanges using Privacy-Enhancing Technologies (PETs). Meanwhile, the Zero-Trust Security Framework enforces stringent access controls, continuously authenticating users and devices to maintain a secure and trustworthy network environment.

The AI-Driven Decision Engine (AID) and Threat Risk Assessor (TRA) complement the orchestration framework by providing contextual insights into threats and vulnerabilities. These components analyze real-time data to prioritize risks and guide the orchestrator in deploying timely and precise mitigation strategies.

PRIVATEER's architecture builds on these principles by integrating privacy-preserving measures into every layer of the network. The Security Orchestration, Automation, and Response (SOAR) component serves as the backbone for automated threat detection and response, ensuring that security protocols can adapt to evolving network conditions. This is complemented by the Level of Trust (LoT) Controller, which evaluates trustworthiness through comprehensive assessments of network integrity, confidentiality, and resilience. To enhance real-time analytics, PRIVATEER deploys AI-driven models at the network edge, enabling anomaly detection and intrusion prevention while preserving user privacy. Federated learning mechanisms further facilitate secure, collaborative threat intelligence sharing, ensuring that sensitive data remains protected during inter-organizational exchanges.

4.3 Impact on 6G and filled security gaps

The contributions of RIGOROUS and PRIVATEER collectively address critical gaps in 6G security and adaptability, ensuring a robust and scalable network infrastructure.

The RIGOROUS project significantly advances the security, scalability, and adaptability of 6G networks by addressing critical gaps in decentralized resource management and dynamic threat mitigation. Its innovative architecture combines advanced orchestration, privacy-preserving frameworks, and zero-trust principles to establish a secure and resilient foundation for next-generation networks.

A cornerstone of RIGOROUS is its AI-Driven Security Orchestrator, which enforces real-time policy adaptation across IoT, RAN, edge, and cloud domains. This orchestration ensures seamless reconfiguration in response to evolving threats, guided by the Threat Risk Assessor, which evaluates vulnerabilities and prioritizes mitigation strategies. The Multi-Cluster Resource Manager further enhances resource allocation and migration by eliminating single points of failure, enabling secure and efficient operations in distributed environments.

RIGOROUS emphasizes privacy through its Privacy-Preserving Cyber Threat Intelligence framework, leveraging advanced technologies to protect sensitive data during collaborative threat analysis. The project also integrates Digital Twin technology to predict and prevent potential disruptions, enabling proactive service reconfiguration and ensuring system resilience. Moreover, its Dynamic and Automatic Service Composition module facilitates seamless integration and interoperability by resolving protocol mismatches and maintaining service continuity in complex scenarios.

By embedding zero-trust principles across its architecture, RIGOROUS enforces strict access controls and continuous authentication, enhancing trust and minimizing vulnerabilities in interconnected systems. The architecture's alignment with regulatory requirements ensures compliance with standards for security, privacy, and transparency, making it a robust solution for the secure operation of 6G networks.

PRIVATEER complements these advancements by focusing on privacy-centric security measures. Its SOAR component enables rapid detection and response to threats while maintaining a focus on lifecycle management. The Level of Trust (LoT) Controller establishes an end-to-end framework for evaluating network integrity, confidentiality, and resilience, addressing gaps in comprehensive trust evaluation. By employing federated learning and edge-based analytics, PRIVATEER ensures that privacy is preserved even during collaborative threat intelligence sharing, enhancing overall system trustworthiness.

The combined impact of these projects creates a 6G ecosystem that is not only adaptive and resilient but also capable of safeguarding privacy and trust. These innovations address pressing challenges such as scalable resource management, real-time threat detection, and user-centric privacy, ensuring that 6G networks meet the diverse demands of next-generation applications while maintaining a robust security posture.

4.4 Recommendations for Decentralized and Adaptive 6G Solutions

To realize the full potential of decentralized and adaptive solutions for 6G, a multi-faceted approach must be adopted, integrating the key advancements and insights from RIGOROUS and PRIVATEER. These strategic recommendations aim to guide future developments:

Enhance Decentralized Protocols Leverage robust decentralized management frameworks, such as those implemented by RIGOROUS, to eliminate single points of failure and ensure scalability. Focus on integrating multi-cluster management systems and smart contracts to foster transparency and automation in resource allocation.

Strengthen Privacy-Preserving Analytics Incorporate privacy-aware orchestration and edge-based analytics to balance performance with user-centric privacy. PRIVATEER's federated learning and secure data sharing models serve as key enablers for this balance, ensuring secure collaboration without compromising sensitive information.

Implement Real-Time Trust and Threat Management Build on adaptive security components like the SOAR system and LoT Controller to maintain dynamic trust evaluations and rapid threat response capabilities. These components should be continuously refined to address emerging threats and enhance the overall trustworthiness of 6G networks.

Prioritize Integration Across the Cloud-Edge-IoT Continuum Develop seamless integration architectures that unify decentralized, privacy-preserving, and adaptive technologies across all layers of the network. The complementary contributions of RIGOROUS and PRIVATEER highlight the need for interoperability and coordination between systems to meet the diverse demands of 6G environments.

Prioritize Integration Across the Cloud-Edge-IoT Continuum Develop seamless integration architectures that unify decentralized, privacy-preserving, and adaptive technologies across all layers of the network. The complementary contributions of RIGOROUS and PRIVATEER highlight the need for interoperability and coordination between systems to meet the diverse demands of 6G environments.

Foster Collaboration and Standardization Encourage cross-domain collaboration and align developments with emerging global standards. This will ensure interoperability, scalability, and consistency in the deployment of decentralized and adaptive 6G solutions.

Invest in Advanced AI and Automation Expand the role of AI-driven security analytics and automation to enhance anomaly detection, intrusion prevention, and resource optimization. The edge-focused deployment of AI/ML models demonstrated by PRIVATEER provides a blueprint for scaling these technologies.

By adopting these recommendations, stakeholders can build resilient and secure 6G networks capable of addressing the dynamic challenges of next-generation communication systems. These strategies ensure that decentralized and adaptive solutions remain at the forefront of innovation, enabling robust, scalable, and user-centric 6G ecosystems.

5 Advanced Technologies for Future-Ready Networks

As the vision for 6G networks evolves, innovative projects like NATWORK and HEXA-X-II address the foundational challenges of security, resilience, and adaptability to meet unprecedented demands. Both projects advance the technological and architectural underpinnings required for next-generation networks by introducing novel concepts and strategies that emphasize robustness, privacy, and trustworthiness.

5.1 Research statement and perspective

The NATWORK project develops a bio-inspired cybersecurity and resilience framework for networking distributed systems that span multiple administrative domains and heterogeneous resources. Drawing an analogy with the human body's immune system, NATWORK employs machine learning (ML) and artificial intelligence (AI) to facilitate real-time security analysis and adaptive responses.

A key focus of NATWORK is on enhancing Physical Layer Security (PLS) as a complementary mechanism to traditional upper-layer security measures. PLS leverages implicit information at the communication level to address wireless communication threats such as jamming, eavesdropping, and sniffing. By utilizing AI-based strategies, the project aims to:

- Develop and validate anti-jamming and attack-detection mechanisms.
- Enhance MIMO and Reconfigurable Intelligent Surface (RIS)-assisted wireless security.
- Introduce Physical Layer Key Generation (PKG) techniques based on channel reciprocity.

NATWORK's contributions extend to creating real-time joint jamming detection and response systems and optimizing RIS configurations through AI, addressing key challenges in 6G frequency bands, multi-antenna systems, and dynamic jamming scenarios.

The HEXA-X-II project is a European flagship initiative that introduces comprehensive design guidelines for 6G end-to-end (E2E) systems. It emphasizes embedding security, privacy, and resilience (SPR) measures as core functionalities across all architectural layers, from infrastructure to application.

Key technological enablers within HEXA-X-II include:

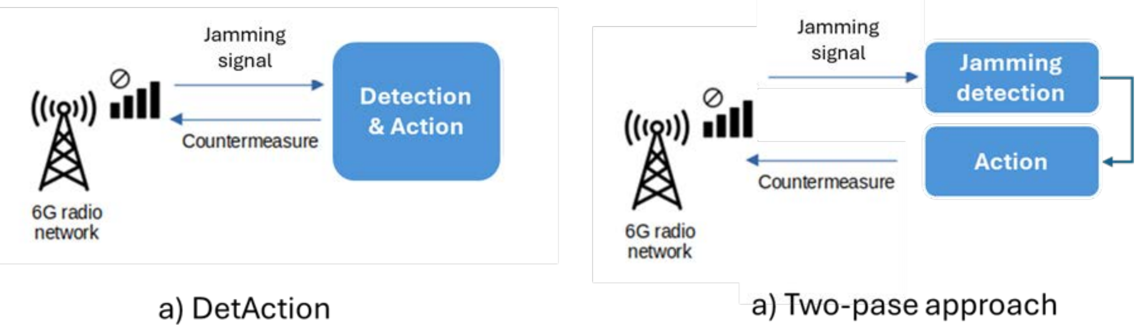
- Zero-trust principles for secure node authentication and interface management.
- Context-aware encryption mechanisms using wireless environmental data for dynamic key generation.
- Physical Layer Deception (PLD) techniques to obstruct eavesdropping by selectively encrypting transmission components.
- Federated Learning (FL) to enhance RAN anomaly detection by enabling distributed model training without centralized data aggregation.
- Post-Quantum Cryptography (PQC) integrated into protocols such as TLS and quantum key distribution (QKD) for quantum-resistant cryptographic solutions.

Additionally, HEXA-X-II addresses the security and privacy of Joint Communication and Sensing (JCAS) data, ensuring compliance with transparency principles and protection against attacks. Its forward-looking approach ensures that 6G networks are prepared to tackle quantum computing threats and other emerging challenges.

5.2 Architecture Innovations and Solutions

The NATWORK and HEXA-X-II projects have introduced transformative architectural innovations to tackle the critical challenges posed by 6G networks. These contributions focus on enhancing resilience, security, and adaptability across multiple network layers, ensuring a robust foundation for next-generation connectivity.

NATWORK presents an innovative AI-driven framework for Physical Layer Security (PLS), designed to provide comprehensive protection against physical-layer attacks. By leveraging advanced techniques, the project offers solutions such as Physical Layer Key Generation (PKG), which utilizes channel reciprocity to enable lightweight and secure key sharing [8]. This mechanism ensures robust encryption and reduces vulnerabilities at the communication level.



a) DetAction

a) Two-pase approach

Figure 7: Anti-jamming system approaches.

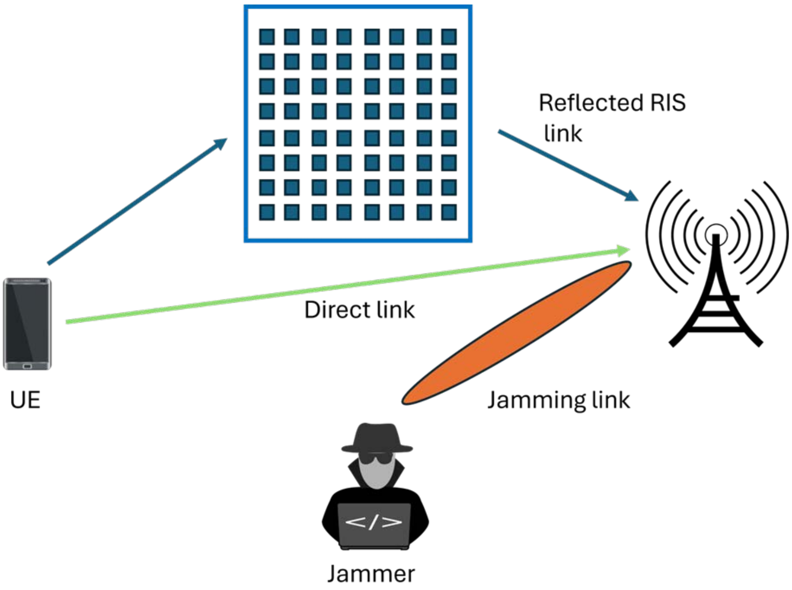


Figure 8: RIS-aided communication system and jamming.

Another critical feature is the real-time joint jamming detection and response system. Through the integration of sophisticated AI models, NATWORK enables rapid identification and mitigation of jamming attacks, safeguarding communication reliability (see Fig. 7). Furthermore, the project incorporates Reconfigurable Intelligent Surface (RIS) and Multiple-Input Multiple-Output (MIMO) technologies, optimized through AI, to protect against sniffing and eavesdropping, as shown in Fig. 8. Together, these innovations create a seamless security continuum that complements traditional measures, enhancing both robustness and efficiency in 6G communication.

HEXA-X-II brings a comprehensive approach to embedding Security, Privacy, and Resilience (SPR) within the architecture of 6G end-to-end systems. The project adopts zero-trust principles to implement rigorous node authentication and secure interface management, ensuring data integrity and confidentiality in disaggregated RAN environments.

Context-aware security is another highlight of HEXA-X-II, utilizing environmental data to dynamically generate encryption keys. This capability allows for adaptive and resilient security protocols that evolve with the network's conditions. Additionally, HEXA-X-II employs Physical Layer Deception (PLD) techniques, which disrupt eavesdropping attempts by selectively encrypting transmission components and applying power-adaptive coding.

The architecture also addresses the dual demands of communication and sensing through Joint Communication and Sensing (JCAS). This ensures secure synchronization, transparency, and user consent for handling sensitive data. HEXA-X-II's emphasis on post-quantum cryptography (PQC) further highlights its forward-looking design, integrating quantum-resistant protocols such as TLS and QKD to safeguard against future threats posed by quantum computing advancements.

5.3 Impact on 6G and filled security gaps

The NATWORK and HEXA-X-II projects play a pivotal role in addressing security gaps and enhancing the robustness of 6G networks by embedding advanced security, privacy, and resilience mechanisms. These initiatives equip 6G networks to tackle emerging challenges, fostering a secure and trustworthy communication ecosystem.

The NATWORK project introduces AI-driven mechanisms to reinforce the physical layer of 6G networks, addressing vulnerabilities inherent to wireless communication. By leveraging anti-jamming measures and RIS-based defense systems, NATWORK provides a security continuum that complements traditional core-focused defenses, enhancing the protection of the radio access network (RAN) and ensuring end-to-end service immunity. This project also pioneers advanced threat modeling tools that precisely identify and mitigate physical-layer vulnerabilities, ensuring robust protection against evolving attacks. Additionally, by integrating Reconfigurable Intelligent Surfaces (RIS) and Multiple-Input Multiple-Output (MIMO) technologies, NATWORK establishes adaptive signal propagation techniques to counter threats like jamming and eavesdropping. These mechanisms, driven by AI, enable dynamic responses to a variety of threats, maintaining both service integrity and user trust.

HEXA-X-II adopts a comprehensive approach to embed Security, Privacy, and Resilience (SPR) measures throughout the 6G architecture, ensuring robust protection across all layers. This project leverages advanced technologies like post-quantum cryptography and federated learning to address critical gaps left by 5G, making 6G systems highly adaptable and trustworthy. HEXA-X-II enhances anomaly detection within disaggregated RAN environments through federated learning, enabling distributed model training without centralized data aggregation. By integrating post-quantum cryptography protocols into standards like TLS, HEXA-X-II ensures resilience against future quantum computing threats. Its approach to securing Joint Communication and Sensing (JCAS) data includes user consent frameworks and protection against jamming and denial-of-service attacks, while context-aware encryption mechanisms dynamically respond to evolving network conditions by utilizing environmental data for adaptive key generation.

5.4 Recommendations for Future Security and Resilience

Building on the significant contributions of the NATWORK and HEXA-X-II projects, the following recommendations aim to guide the development and deployment of advanced technologies for future-ready 6G networks. These strategies integrate insights from the unified visions and project contributions to ensure robust, adaptive, and scalable solutions.

Enhance Physical Layer Security and AI Integration
Strengthen physical layer defenses by integrating advanced AI mechanisms, such as those developed in NATWORK, to dynamically detect and respond to threats like jamming and eavesdropping. The adoption of Reconfigurable Intelligent Surfaces (RIS) and Multiple-Input Multiple-Output (MIMO) technologies should be further expanded, with optimized configurations driven by AI to maximize signal security and adaptability in diverse environments.

Embed Security, Privacy, and Resilience as Core Principles
Leverage HEXA-X-II's approach to embedding Security, Privacy, and Resilience (SPR) measures throughout the network architecture. This includes incorporating zero-trust principles for secure node authentication and dynamic context-aware encryption mechanisms that adapt to changing environmental conditions. Ensuring these principles are intrinsic to system design will create a more resilient and trustworthy 6G ecosystem.

Advance Quantum-Resistant Cryptographic Solutions
Prepare 6G networks for quantum computing threats by integrating post-quantum cryptographic protocols, as demonstrated in HEXA-X-II. Expand the deployment of quantum-safe standards such as TLS and QKD, ensuring that critical data and communication channels remain secure against evolving technological capabilities.

Foster Federated Learning and Distributed Security Models
Promote federated learning and decentralized security frameworks to enhance anomaly detection and real-time threat management. By enabling secure model training without centralized data aggregation, as demonstrated in both projects, networks can scale effectively while preserving data privacy and confidentiality.

Develop Adaptive Integrated Sensing and Communication (ISAC) Protocols
Expand the use of ISAC systems to ensure secure and efficient synchronization and data handling. Build on HEXA-X-II's user-consent frameworks and context-aware encryption to align with transparency principles and enhance protection against jamming and denial-of-service attacks.

Prioritize Real-Time Threat Mitigation Strategies
Ensure the development of AI-driven, real-time threat mitigation mechanisms, leveraging the dynamic adaptability seen in NATWORK's anti-jamming and attack response systems. These solutions should be seamlessly integrated into both the physical and application layers to maintain network integrity under evolving conditions.

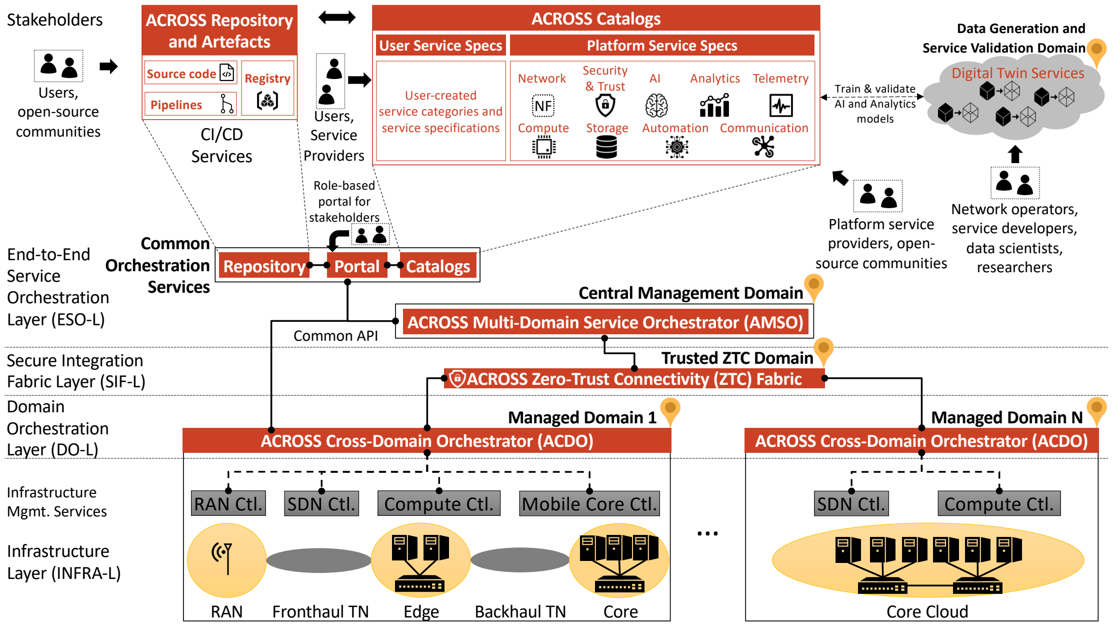

Stakeholders
Users, open-source communities
ACROSS Repository and Artefacts
Source code
Registry
Pipelines
CI/CD Services
Users, Service Providers
ACROSS Catalogs
User Service Specs
Platform Service Specs
User-created service categories and service specifications
Network
Security & Trust
AI
Analytics
Telemetry
NF
Compute
Storage
Automation
Communication
Data Generation and Service Validation Domain
Digital Twin Services
Train & validate AI and Analytics models
Role-based portal for stakeholders
Platform service providers, open-source communities
Network operators, service developers, data scientists, researchers
End-to-End Service Orchestration Layer (ESO-L)
Common Orchestration Services
Repository
Portal
Catalogs
Central Management Domain
ACROSS Multi-Domain Service Orchestrator (AMSO)
Common API
Secure Integration Fabric Layer (SIF-L)
Trusted ZTC Domain
ACROSS Zero-Trust Connectivity (ZTC) Fabric
Domain Orchestration Layer (DO-L)
Managed Domain 1
ACROSS Cross-Domain Orchestrator (ACDO)
Managed Domain N
ACROSS Cross-Domain Orchestrator (ACDO)
Infrastructure Mgmt. Services
RAN Ctl.
SDN Ctl.
Compute Ctl.
Mobile Core Ctl.
SDN Ctl.
Compute Ctl.
Infrastructure Layer (INFRA-L)
RAN
Fronthaul TN
Edge
Backhaul TN
Core
...
Core Cloud

Figure 9: Overview of the ACROSS platform architecture.

Drive Collaboration and Standardization
Foster collaboration between research initiatives, industry stakeholders, and policymakers to align technological advancements with global standards. Such efforts will enable interoperability, ensure scalability, and streamline the deployment of innovative solutions across diverse regions and applications.

By embracing these recommendations, stakeholders can establish a resilient, secure, and scalable 6G ecosystem capable of addressing the complex challenges of next-generation communication networks. NATWORK and HEXA-X-II provide a robust blueprint for future efforts, demonstrating how innovative technologies and architectural frameworks can drive the transformation toward advanced, future-ready networks.

6 Scalable and Zero-Touch Approaches

The need for scalable, automated, and user-centric solutions in 6G networks drives the innovative efforts of the ACROSS and 6G-BRICKS projects. Both projects emphasize frameworks and technologies designed to simplify and secure complex network environments while ensuring adaptability and resilience.

6.1 Research statement and perspective

The ACROSS project envisions a secure, scalable platform that seamlessly manages complex network services across distributed edge-to-core deployments (see Fig. 9 for an overview). ACROSS introduces a Zero-Touch service provisioning framework that eliminates manual intervention, enhancing automation and efficiency. The core of ACROSS lies in its robust security and trust services, which include:

- Remote Attestation: Continuous integrity verification of domain nodes and containers, ensuring only trusted resources participate in service provisioning. This mechanism uses Trusted Platform Modules (TPMs) and the Integrity Measurement Architecture (IMA) to attest the software stack and runtime environments.
- Dynamic Service Management: The platform provides automatic migration of containers from compromised nodes, maintaining service integrity and availability. This feature ensures that only healthy nodes host critical services, even in distributed and dynamic scenarios.
- Network Digital Twins (NDTs): NDTs are leveraged for realistic dataset generation, AI model validation, and optimization of service deployment strategies. This enables predictive maintenance and preemptive security measures.

The 6G-BRICKS project focuses on integrating Software-Defined Perimeters [5] (SDP) and Zero Trust [10] (ZT) architectures to create a dynamic and secure network environment. Its contributions center around scalable security management frameworks designed to meet the evolving needs of 6G systems. Key innovations include:

- Security Intents: High-level abstractions used to define and enforce security policies dynamically. These intents simplify network security management by bridging the gap between operators and practitioners, enabling automated security processes in Zero-Touch environments.
- Multi-Tier Security Management: The integration of SDP controllers and service security orchestrators ensures tailored security mechanisms, such as VPN-as-a-Service and granular access controls, that adapt to specific endpoints and resources.
- Policy-Based Management: Dynamic configuration and enforcement of security measures in data planes, ensuring seamless adaptation to new threats and requirements.

6.2 Architecture Innovations and Solutions

The ACROSS and 6G-BRICKS projects represent a significant step forward in designing scalable and automated solutions for secure and resilient 6G networks. Both initiatives address the challenges of cross-domain service management and integrate advanced security architectures, offering complementary innovations to meet the demands of next-generation network infrastructures.

The ACROSS project introduces a secure, zero-touch service orchestration platform to manage complex network services across distributed environments. A central feature is its remote attestation framework, which employs Trusted Platform Modules (TPMs) and the Integrity Measurement Architecture (IMA) to ensure the integrity of domain nodes and containers. This system verifies compute resources at initialization and during runtime, ensuring that only trustworthy nodes host service containers. If a node is compromised, the framework automatically migrates containers to healthy nodes, preserving service integrity and availability.

Network Digital Twins (NDTs) play a pivotal role within the ACROSS architecture, generating realistic datasets, validating AI models, and optimizing service deployments. By offering predictive capabilities, these digital twins enhance the platform's ability to identify potential threats and preemptively secure network operations. Furthermore, the platform's approach to dynamic container management, distinguishing between stateless and stateful containers, enables secure migration processes while preserving continuity in dynamic and heterogeneous environments.

The 6G-BRICKS project complements ACROSS with its robust security management framework that incorporates ZT principles and implement an SDP-centric environment. It emphasizes security intents, which are high-level abstractions allowing operators to define and enforce dynamic security policies. Such intents, based on these defined by TMF for network management [1], simplify interactions between network operators and security mechanisms, streamlining security management in cloud-native and multi-domain environments.

Central to 6G-BRICKS' architecture [4] (Fig. 10) is its multi-tiered security management approach. By integrating an SDP Controller and service security orchestrators, the framework provides granular control over configurations such as VPN-as-a-Service (VPNaaS) and SDP Gateways. This flexibility enables the framework to dynamically adapt to specific user and application requirements, ensuring fine-grained access control and secure communication channels. The architecture's policy-based mechanisms automate security configuration and adaptation, enabling real-time responses to evolving threats and seamless enforcement of tailored security measures.

6.3 Impact on 6G and filled security gaps

The ACROSS and 6G-BRICKS projects address key security challenges of 6G networks, filling critical gaps in scalability, automation, and trustworthiness. By introducing cutting-edge technologies and frameworks, these initiatives ensure that 6G networks can dynamically respond to emerging threats and maintain operational integrity in diverse environments.

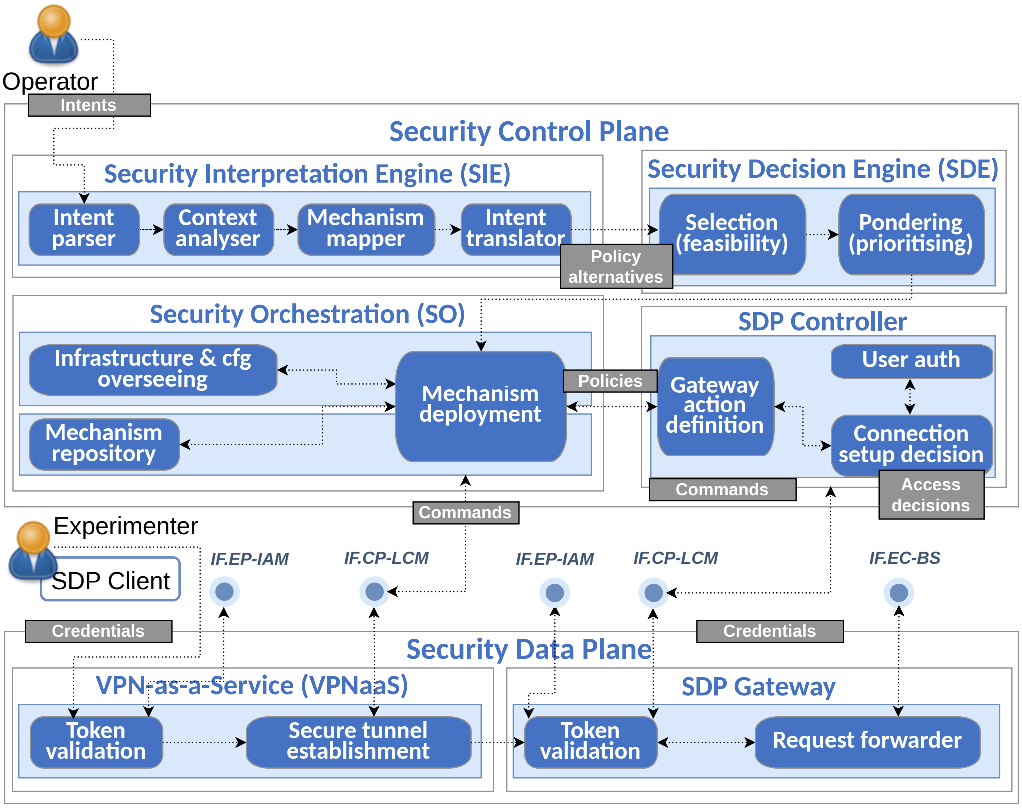


Figure 10: 6G-BRICKS Security Architecture.

ACROSS emphasizes the importance of remote attestation, a cornerstone of trusted computing, to secure shared compute resources. This capability is integrated into the platform core, ensuring that physical nodes, virtual machines, and containers are continuously verified for integrity. This approach provides scalable and seamless service deployments, where container attestation plays a critical role in securing the 6G platforms and the network services they host.

A notable contribution of ACROSS is the OpenSTO architecture, which decentralizes Zero-Touch Service Management (ZSM) Closed Loop (CL) processes (see Fig. 11). This decentralization reduces the burden on central elements, enhancing scalability and minimizing downtime during upgrades. The architecture's modularity allows tasks like data collection and analysis to occur closer to data plane resources, improving real-time threat detection and resource management.

The use of Network Digital Twins (NDTs) enhances the ability to simulate, validate, and optimize services in virtual environments. These twins are instrumental in generating realistic datasets for AI models, enabling advanced attack detection and mitigation strategies tailored to the dynamic nature of 6G networks. By embedding adaptive cybersecurity measures, ACROSS ensures the network can anticipate and counter novel threats effectively.

The 6G-BRICKS project introduces a robust framework that aligns with the principles of ZT and SDP. Security intents bridge the gap between high-level oper-

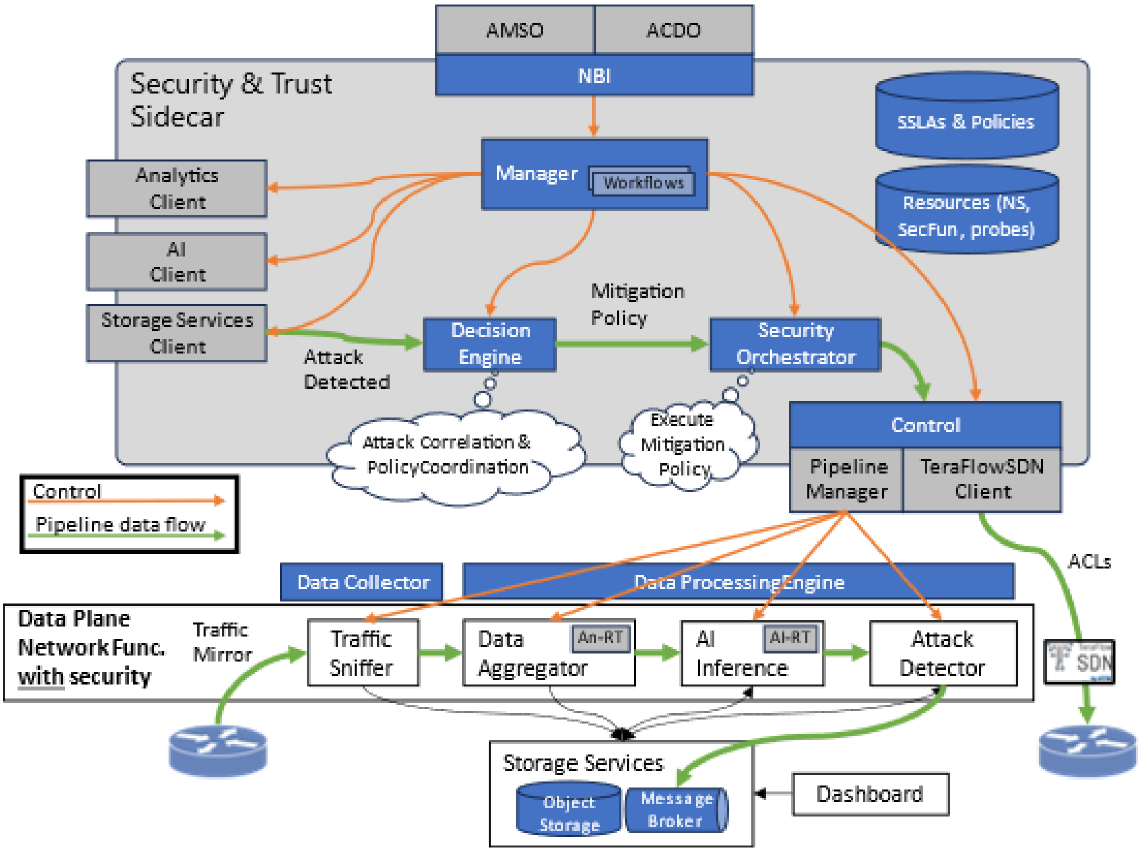


Figure 11: Overview of the Open Security and Trust Orchestrator (OpenSTO).

ational requirements and the technical deployment of security measures. This innovation simplifies the management of security policies, enabling automated and precise enforcement of access controls and configurations.

By incorporating intent-driven policy-based management, 6G-BRICKS provides tailored security solutions that adapt dynamically to evolving network conditions. Its SDP architecture enhances granular control over endpoints, establishing secure tunnels and fine-grained access to protected resources. These mechanisms ensure a resilient and scalable security framework that addresses gaps in traditional cloud-native environments.

The project also leverages a Security-as-a-Service (SECaaS) approach, providing flexible and automated responses to security requirements. This strategy ensures seamless protection in multi-stakeholder scenarios, where operators interact with dynamic groups of verticals and security providers. By focusing on adaptability and precision, 6G-BRICKS enhances the efficiency of security operations in complex environments.

6.4 Recommendations for Future Security and Automation

Building on the significant contributions of ACROSS and 6G-BRICKS, it is clear that scalable and zero-touch solutions are essential to the future of 6G networks. Advanced remote attestation frameworks, such as those demonstrated in

ACROSS, must be integrated across all layers of 6G architectures to continuously verify the integrity of physical nodes, virtual machines, and containers. This will ensure service reliability and secure distributed resources in dynamic environments. Automating these processes can further reduce operational overhead and enhance scalability.

Zero Trust architectures and intent-driven security management frameworks, as exemplified by 6G-BRICKS, should be widely adopted to enable precise and automated enforcement of access controls and configurations. Security intents can bridge the gap between operational requirements and technical deployment, ensuring seamless management of policies in cloud-native and multi-domain environments. These principles should extend to edge, core, and cloud systems for a comprehensive security posture.

The use of Network Digital Twins (NDTs) must be expanded to simulate, validate, and optimize services in virtual environments. Building on ACROSS's contributions, NDTs should be integrated into cybersecurity frameworks to provide predictive capabilities for preemptive threat mitigation and dynamic adaptation to new attack vectors. These tools are also invaluable in training AI models for anomaly detection and response, enhancing overall network security.

Policy-based security management and Security-as-a-Service (SECaaS) models, as demonstrated in 6G-BRICKS, are vital for automating and simplifying security operations. Flexible and tailored security solutions can adapt to multi-stakeholder environments, addressing the specific needs of diverse verticals and operators. These approaches ensure real-time enforcement and adaptation to changing conditions, enabling a resilient and responsive security framework.

The development of modular and decentralized architectures, such as the Open-STO approach in ACROSS, is crucial to enhancing scalability and resilience. Decentralized architectures reduce the burden on central elements, improve real-time resource management, and support incremental upgrades without disrupting existing operations. Modular designs also allow seamless integration of emerging technologies.

Collaboration among industry stakeholders, research initiatives, and policymakers must be encouraged to align the development of scalable and zero-touch solutions with global standards. Such alignment will ensure interoperability, streamline deployment, and facilitate the adoption of innovative frameworks across diverse regions and applications.

The expansion of AI-driven automation is another cornerstone of these recommendations. Real-time responses to emerging threats can be achieved through AI models for anomaly detection, container migration, and policy enforcement. Both ACROSS and 6G-BRICKS emphasize the importance of dynamic adaptability in security frameworks, and AI should be leveraged to continuously refine protocols and optimize network performance.

7 Key Innovations Across SNS Projects for 6G Development

The following table highlights the key innovations introduced by various SNS projects, demonstrating their significant contributions to the development of scalable, secure, and resilient 6G networks.

Innovation	**SNS Project(s)**
AI-driven architectures for dynamic trust evaluation and continuous security validation	DESIRE-6G, iTrust6G, RIGOROUS
Holistic trustworthiness framework integrating safety, security, privacy, resilience, and reliability	SAFE-6G
Blockchain-enabled mutual remote attestation (D-MUTRA)	DESIRE-6G
Zero-touch service provisioning and security validation across heterogeneous environments	DESIRE-6G, ACROSS
Dynamic service topology adaptation with modular trust frameworks	iTrust6G, RIGOROUS
AI-enhanced threat detection and classification using federated learning	iTrust6G, PRIVATEER, HEXA-X-II, RIGOROUS
Bio-inspired cybersecurity and resilience framework leveraging AI for real-time adaptive responses	NATWORK
Physical Layer Security (PLS) enhancements using MIMO and Reconfigurable Intelligent Surfaces (RIS)	NATWORK
Post-Quantum Cryptography (PQC) and federated learning for anomaly detection	HEXA-X-II, NATWORK
Privacy-friendly Cyber Threat Intelligence (CTI) sharing with federated learning and homomorphic encryption	PRIVATEER, HEXA-X-II, RIGOROUS
Zero-trust principles and context-aware encryption mechanisms for node authentication and interface management	HEXA-X-II, 6G-BRICKS, RIGOROUS, iTrust6G
Security Intents for dynamic policy enforcement in zero-touch environments	6G-BRICKS, ACROSS
Network Digital Twins (NDTs) for AI model validation and predictive maintenance	ACROSS, DESIRE-6G
Remote attestation frameworks ensuring cross-domain service integrity	ACROSS, DESIRE-6G, RIGOROUS
Decentralized privacy-aware orchestration and resource management	RIGOROUS, PRIVATEER

Physical Layer Deception (PLD) to counter eavesdropping	HEXA-X-II
Security-as-a-Service (SECaaS) for automated security operations	6G-BRICKS, PRIVATEER

Table 1: Innovations Across SNS Projects for 6G Development

8 CONCLUSIONS

This paper presents a comprehensive analysis of the security, trust, and privacy challenges in the 6G landscape, alongside innovative solutions to address them. The envisioned 6G systems must operate in dynamic and heterogeneous environments, requiring trustworthiness to be embedded as a native feature. By balancing safety, security, privacy, resilience, and reliability, the proposed solutions cater to diverse stakeholder needs and ensure operational flexibility.

Artificial intelligence and machine learning are pivotal in advancing 6G security, enabling real-time threat detection, dynamic trust evaluation, and adaptive responses. Projects like iTrust6G and NATWORK demonstrate the potential of intelligent systems to enhance decision-making and secure next-generation infrastructures.

Decentralized and scalable architectures, such as those proposed in RIGOROUS and ACROSS, provide robust frameworks for secure resource management across distributed environments. The ACROSS project also incorporates Network Digital Twins (NDTs), which serve as a key enabler for realistic dataset generation, AI model validation, and service optimization. This innovation enhances the ability to simulate complex scenarios, ensuring better preparedness and adaptability for 6G systems.

Privacy remains a cornerstone of 6G security. PRIVATEER underscores the importance of privacy-first architectures, integrating privacy-aware orchestration and secure threat intelligence sharing to ensure compliance with regulations while fostering trust. Similarly, forward-looking technologies like post-quantum cryptography and federated learning, as demonstrated in Hexa-X-II and NATWORK, prepare 6G networks to withstand both current and emerging threats.

Together, these solutions establish a foundation for secure, adaptive, and resilient 6G systems, addressing critical gaps in existing frameworks while meeting the demands of an increasingly complex digital future.

References

[1] Intent in autonomous networks v1.3.0 (ig1253). Technical report, Telemanagement Forum, August 2022.

[2] Muhammad Asad, Ahmed Moustafa, and Takayuki Ito. Federated learning versus classical machine learning: A convergence comparison. *arXiv preprint arXiv:2107.10976*, 2021.

[3] Maxime Compastié, Rémi Badonnel, Olivier Festor, and Ruan He. From virtualization security issues to cloud protection opportunities: An in-depth analysis of system virtualization models. *Computers & Security*, 97:101905, October 2020.

[4] Carolina Fernández-Martínez, Anastasios Bikos, Christos Verikoukis, and Shuaib Siddiqui. Trusted access to 6g testbeds through a security intent-driven software-defined perimeter framework. *Zenodo preprint 10.5281/zenodo.13626977*, September 2024.

[5] Jason Garbis, Juanita Koilpillai, Junaid Islam, Bob Flores, Daniel Bailey, Benfeng Chen, Eitan Bremler, Michael Roza, and Ahmed Refaey Hussein. Software-defined perimeter (sdp) specification v2.0. Technical report, Cloud Security Alliance, March 2022.

[6] Mir Ghoraishi, Muhammad Shuaib Siddiqui, Maxime Compastie, Saber Mhiri, Christos Ntanos, Michael Kontoulis, Diego Lopez, Antonio Lioy, Evangelos K. Markakis, and Sheeba Backia Mary Baskaran. iTrust6G: Zero-Trust security for 6G networks. In *2024 IEEE Future Networks World Forum (FNWF) (FNWF'24)*, page 6, Dubai, United Arab Emirates, October 2024.

[7] Ryuta Kremer, Prasanna N Wudali, Satoru Momiyama, Toshinori Araki, Jun Furukawa, Yuval Elovici, and Asaf Shabtai. Ic-secure: Intelligent system for assisting security experts in generating playbooks for automated incident response. *arXiv preprint arXiv:2311.03825*, 2023.

[8] Guyue Li, Chen Sun, Junqing Zhang, Eduard Jorswieck, Bin Xiao, and Aiqun Hu. Physical layer key generation in 5g and beyond wireless communications: Challenges and opportunities. *Entropy*, 21(5):497, 2019.

[9] Mohammad Moshawrab, Mehdi Adda, Abdenour Bouzouane, Hussein Ibrahim, and Ali Raad. Reviewing federated learning aggregation algorithms; strategies, contributions, limitations and future perspectives. *Electronics*, 12(10):2287, 2023.

[10] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly. Zero Trust Architecture. Technical report, National Institute of Standards and Technology, August 2020.

9 ABBREVIATIONS AND ACRONYMS

Abbreviation	Description
6G	Sixth Generation (mobile networks)
AAA	Authentication, Authorization, and Accounting
AI	Artificial Intelligence
AIMLF	AI/Machine Learning Framework
DLT	Distributed Ledger Technology
D-MUTRA	DLT-Mutual Remote Attestation
E2E	End-to-End
GDPR	General Data Protection Regulation
IDAN	Intent-Driven Autonomous Networks
IoC	Indicators of Compromise
IoT	Internet of Things
ISAC	integrated Sensing and Communications
KPI	Key Performance Indicator
LoT	Level of Trust
ML	Machine Learning
MLFO	Machine Learning Function Optimizer
MIMO	Multiple-Input, Multiple-Output
NWDAF	Network Data Analytics Function
PQC	Post-Quantum Cryptography
PLD	Physical Layer Deception
PKG	Physical Layer Key Generation
QoS	Quality of Service
RAN	Radio Access Network
RIS	Reconfigurable Intelligent Surface
SBA	Service-Based Architecture
SECaaS	Security as a Service
SDS	Software-Defined Security
SDN	Software-Defined Networking
SDP	Software-Defined Perimeters
SLA	Service Level Agreement
SMO	Service Management and Orchestration
SON	Self-Organising Networks
SoTA	State of the Art
TDD	Time Division Duplexing
TMF	Telemanagement Forum
TOSCA	Topology and Orchestration Specification for Cloud Applications
TPM	Trusted Platform Module
UE	User Equipment
VM	Virtual Machine
ZT	Zero Trust
ZSM	Zero-Touch Service Management

10 CONTACTS

WG Chair:
Pascal Bisson, Thales, HE SNS ROBUST-6G and HE SNS SAFE-6G
pascal.bisson@thalesgroup.com

WG Co-chair:
Antonio Skarmeta, Universidad de Murcia, HE SNS RIGOROUS
skarmeta@umu.es

SNS WGs:
https://6g-ia.eu/6g-ia-working-groups/#security

11 LIST OF EDITORS

Name	Institution	Country	Project
Noelia Pérez Palma	University of Murcia	Spain	HE SNS HEXA-X-II
Antonio Skarmeta	University of Murcia	Spain	HE SNS RIGOROUS
Pascal Bisson	Thales	France	HE SNS ROBUST-6G, HE SNS SAFE-6G

12 LIST OF CONTRIBUTORS

Contributor	SNS Project
Vincent Lefebvre - Sarl Tages SOLIDSHIELD, France	HE SNS DESIRE-6G
Carlos Jesus Bernardos Cano - UC3M University, Spain	HE SNS DESIRE-6G
Luis Velasco - UPC Polytechnic University of Catalonia, Spain	HE SNS DESIRE-6G
Carolina Fernández - i2CAT Foundation & Pompeu Fabra University, Spain	HE SNS 6G-BRICKS
Maxime Compastié - i2CAT Foundation, Spain	HE SNS iTrust6G
Ioannis Xidias - National Technical University of Athens, Greece	HE SNS iTrust6G
Lorenzo Ferro - Politecnico di Torino, Italy	HE SNS iTrust6G
Felix Klaedtke – NEC Laboratories Europe, Germany	HE SNS ACROSS
Pol Alemany – CTTC, Spain	HE SNS ACROSS
Lluís Gifre – CTTC, Spain	HE SNS ACROSS
Ricard Vilalta – CTTC, Spain	HE SNS ACROSS
Raul Muñoz – CTTC, Spain	HE SNS ACROSS
Antonio Pastor – Telefonica, Spain	HE SNS ACROSS
Georgios Gardikis – Space Hellas, Greece	HE SNS PRIVATEER
Maria Christopoulou – NCSR ”Demokritos”, Greece	HE SNS PRIVATEER
Joaquín Escudero – GRADIANT, Spain	HE SNS NATWORK
Pawani Porambage – VTT Technical Research Centre, Finland	HE SNS HEXA-X-II
Diego R. López – Telefónica, Spain	HE SNS HEXA-X-II, HE SNS iTrust6G
Harilaos Koumaras – NCSR ”Demokritos”, Greece	HE SNS SAFE-6G
Spyridon Georgoulas – NCSR ”Demokritos”, Greece	HE SNS SAFE-6G
Christos Xenakis – INQBIT INNOVATIONS SRL (IQBT)	HE SNS SAFE-6G