Zero-Touch Network and Service Management (ZSM) in 6G: A Comprehensive Roadmap From Theory to Deployment

Saher Pervaiz [1], Sonia Shahzadi [2], Anwer Al-Dulaimi [3], Chih-Lin I [4]
[1]Department of Computer Science, University of The Chenab, Pakistan
[2]Department of Computer Science, Air University, Pakistan
[3]Veltris & Zayed University, Canada
[4]China Mobile Research Institute, Beijing, China

Zero-Touch Network and Service Management (ZSM) is needed for the automation, resilience, and intention-driven agility of future networks, particularly in 6G. ZSM intends to deliver end-to-end, AI-enabled orchestration of AI without various management domains and across diverse settings with minimal human participation, in contrast to the management paradigms in 5G. For this reason, we attempt to draw a bridge from theory to practical implementation by integrating fundamental concepts to practical challenges in the field of basic technologies, novel architecture, and frameworks in the ZSM, which is a crucial 6G network enabler. In the synthesis of advanced solutions, we attempt to analyze the literature on uneven scales, contradictory frameworks, and reference the gaps in reproducibility, latency trade-offs, federated and reinforcement learning, purpose ambiguity, privacy, and the overemphasized imperative of scalability. To facilitate our synthesis, we define a taxonomy, provide the standards for comparative evaluation, and reclaim a methodology for future work. Lastly, we provide research on the intersection of advanced automation and ZSM theories, focusing on conflict-aware automation, intent semantic standardization, and edge deployment of AI models to propel forward areas such as quantum-resilient automation.

***Index Terms*—Zero touch, 5G, 6G, Artificial intelligence, Machine learning, Intent-based AI, Reinforcement learning, Federated learning, Network automation, Network orchestration, Network slicing, Service lifecycle management, Blockchain, Edge computing, Autonomous networks, Network security.**

I. Introduction

Shifting from fifth-generation (5G) networks to sixth-generation (6G) networks not only signifies advancement within wireless communication but also marks new ways of network management, automation, and deployment. 5G brought mobile broadband (eMBB), ultra-reliable low-latency communications (URLLC), and massive machine type communications (mMTC), while 6G begins to emerge and demands full mesh network automation, self-optimization, and end-to-end orchestration. In this regard, Zero-Touch Network and Service Management (ZSM) is a primary enabling technology which moves from automation theoretical models to models of pragmatic automation within multi-domain, multi-technology, and heterogeneous domain environments. Autonomous vehicles, smart factories, extended reality environments, and real-time telemedicine, and any other such applications need ZSM to achieve fast extreme automation, multi-domain controlled scalability, and high domain resilience with little human control.

Further highlighting these changes, Zero Touch Network and Service Management is gaining attention aimed at end-to-end automation of the entire service lifecycle with little human input [1]. Such a trend also places greater focus on advanced security frameworks. As outlined in [2], zero trust security frameworks are becoming a necessity in 5G and 6G systems to protect open and distributed infrastructures via continuous monitoring and dynamic policy enforcement. Artificial intelligence is a constituent element in the zero touch architecture. In Open RAN environments, Federated Learning and Deep Reinforcement Learning are used as discussed in [3] to assist in distributed decision making and coordination for a team of agents. These techniques are important in managing cross domain vendor and technology neutral networks. These approaches give support to empirical research. For instance, [4] performs an experimental study on zero-touch orchestration in Beyond 5G scenarios. This illustrates machine intelligence's capacity to convert high-level intents into self-optimizing flows. With respect to security scenarios, automated machine learning is gaining prominence in threat detection as well as dynamic real-time measurements [5]. These initiatives are tied on core technologies such as software-defined networking (SDN), network function virtualization (NFV), and multi-access edge computing (MEC). These technologies together facilitate the closed-loop automation and intelligent control necessary for multi-level automated and adaptive network management [6]. The ACROSS system described in [7], is an architecture of a cross-layer end-to-end 5G vertical application automation service provisioning platform. Such frameworks show that by incorporating intent intented policies with AI automation, human-centric workflows can become more efficient and reliable. The automation movement driven by artificial intelligence also has to consider emerging security challenges. For instance, in federated learning frameworks for distributed intelligence in zero-touch networks, the frameworks are susceptible to poisoning attacks which can drastically undermine the reliablity of the overall system. Corresponding protective measures

such as secure aggregation and anomaly intrusion detection, as described in [8], have been developed in response to impose these frameworks. ZSM still requires automation to support effective lifecycle management as described in [9]. This automates integration, observation, augmentation, and gradual termination of hybrid networks. Purposeful orchestration means less attention orchestration on manual tasks. Virtualisation enables autonomy. Apparently easier self-sufficient systems requires more control and guide to mechanism as indicated in [10]. Another crucial issue is that of security, particularly concerning the edge. Consumer grade edge nodes and software-defined infrastructures are being studied by [11], which focuses on building IoT security frameworks. These seek to incorporate security at the foundational level of distributed control system architecture. The scope of security orchestration is expanding to embrace an increasing number of disciplines. [12] provides an extensive study of multi-domain orchestration and enumerates the integration issues it attempts to resolve, alongside the consolidated control infrastructures it offers. This is further augmented by intent-based networking frameworks, which translate organizational objectives into appropriate network governance [13]. Implementation of the zero trust security framework still remains a relevant topic in ZSM. The detailed analysis presented in [14], emphasizes, in particular, the continuous verification and least privileged access aspects, the implementation of automated network administration and the integration of zero trust values. The advancement of zero touch systems pays more and more attention to Quality of Experience in the network. [15], for instance, proposes a hybrid framework of machine learning for optimizing network user experience and video streaming services over 5G. The same stream of research is also concerned with the efficient and effective distribution of resources. [16] describes the autonomous services provisioning communication and computation resources allocation optimization techniques in large scale cell-free IoT networks. Practical implementations are finally starting to take shape. The Smart Highway Testbed in [17] showcases the use of Zero Touch Network and Service Management with the orchestration of edge and mobile nodes for vehicle services, and also the resource management.

This review synthesizes research from 2021 to 2025 to answer five primary questions:

RQ1: Which architectural frameworks facilitate intent based automation in ZSM for 5G/6G, and what are their incorporate intent intent exposure, translation, and enforcement layers?

RQ2: What role do Artificial Intelligence and Machine Learning play in intent parsing, conflict resolution, and enforcement in ZSM closed loop systems?

RQ3: In what ways do mechanisms for security and privacy of translation and execution of intent in ZSM for multiple domains integrate with zero trust, blockchain and explainable AI to strengthen trust, and how do these systems augment intent based automation?

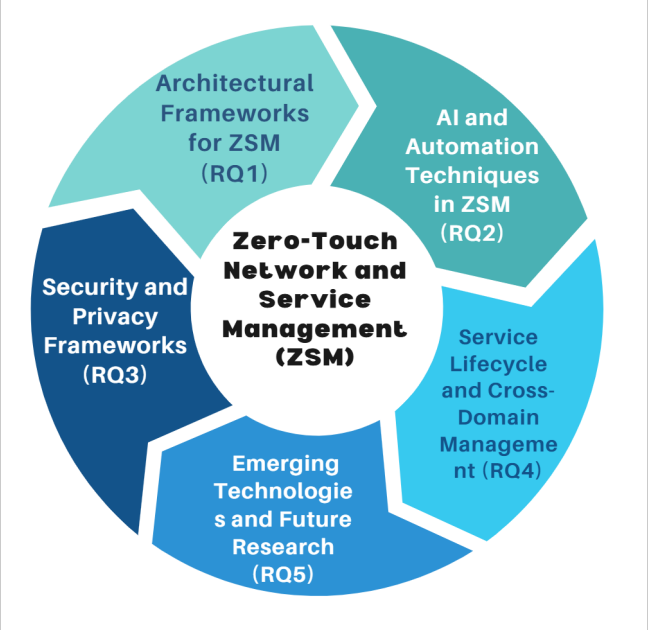

Fig. 1: Research questions guiding the survey on Zero-Touch Network and Service Management (ZSM) in 5G and 6G networks. The five questions (RQ1–RQ5) address key aspects, including architectural frameworks, AI/ML techniques, security and privacy mechanisms, service lifecycle management, and emerging challenges and future directions. These questions structure the comprehensive review and analysis of 128 selected studies from 2021–2025, covering intent-driven automation, cross-domain orchestration, and trustworthy autonomous network management.

RQ4: How can intent driven orchestration enhance service lifecycle management (on-boarding, assurance, scaling, and decommissioning) across heterogeneous domains in 6G networks?

RQ5: What are the open challenges and future research directions for intent based automation in ZSM, particularly regarding semantic standardization, real-time translation, interoperability, and explainability?

This paper aims to offer a foundational reference for researchers and practitioners working on secure, scalable, and autonomous zero-touch management systems for next-generation networks.

II. State of the Art

An expanding body of work on Zero-Touch Network and Service Management spans architectural frameworks, AI-driven orchestration, security and privacy, lifecycle of MLOps, and vertical deployments. Building on our systematic review of 128 studies, we synthesize the literature into five themes aligned with our research questions (RQ1–RQ5). To keep the narrative tightly coupled to evidence, Tables I–VIII provide structured single-reference comparisons (Key Attributes, Strengths, Limitations), while Fig. 3 summarize temporal trends and topical coverage.

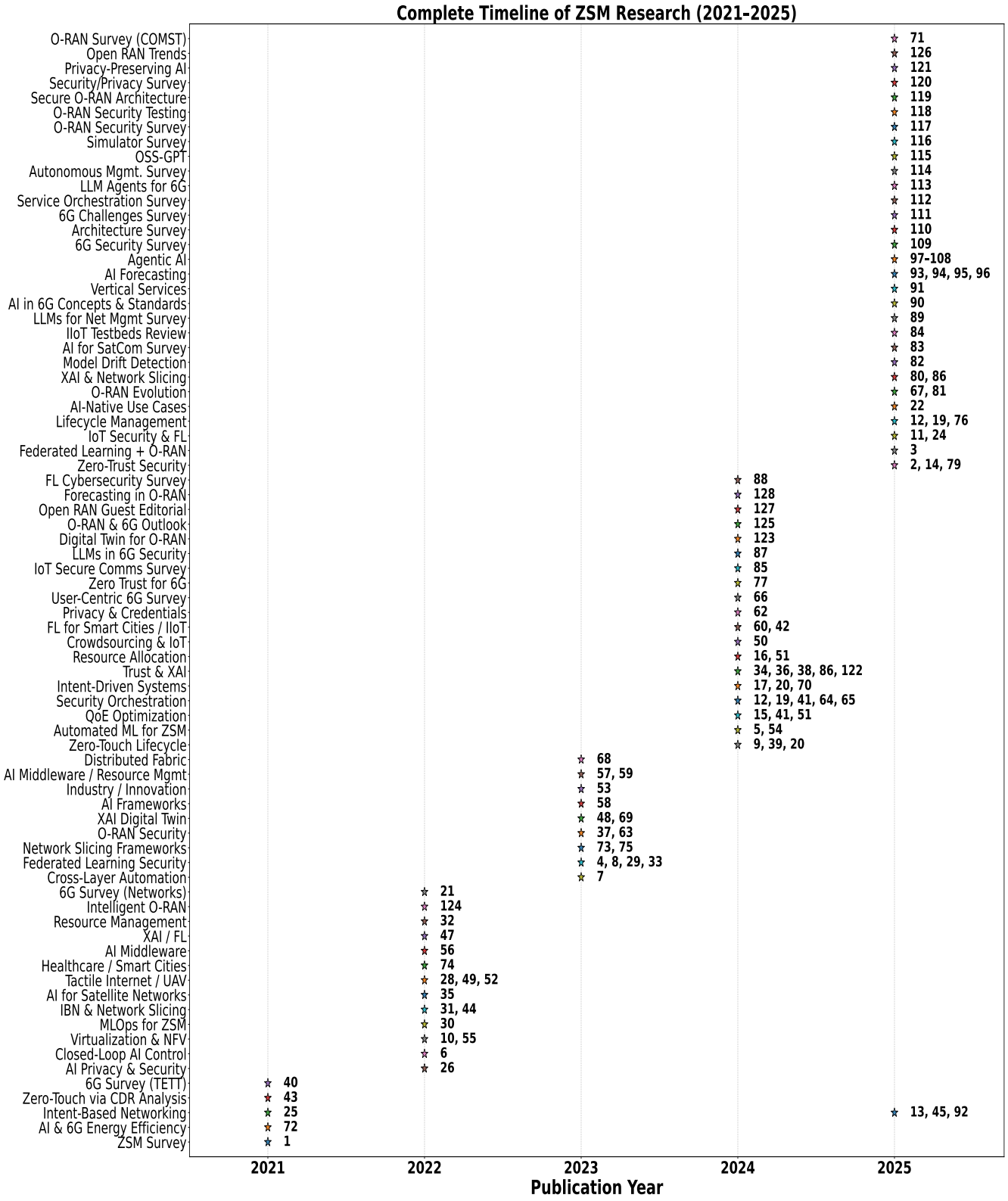

Fig. 2: Research on ZSM has grown exponentially, with major emphasis on AI-driven orchestration after 2023.

TABLE I Critical Analysis of ZSM Research Based on Single Reference

References	Category	Key Attributes	Strengths	Limitations	Critical Insight
[1]	Survey on ZSM	Broad review of NFV, SDN, MANO automation	Provides taxonomy, structured overview	Lacks benchmarks, 6G vision shallow	Baseline survey; outdated for AI-native orchestration.
[2]	Zero-Trust Security	ZTA with continuous authentication in 5G+	Defines threat/control model	No testbed or deployment	Conceptual only; integration in multi-domain still open.
[3]	Federated DRL (O-RAN)	FL + DRL for O-RAN reconfiguration	Scalable coordination, adaptive learning	High training/comm. cost, no real O-RAN testbed	Promising but impractical without efficient FL compression.
[4]	Experimental ZSM	Testbed orchestration	Provides real measurement data	Narrow vendor scope, small-scale	Rare empirical validation but lacks reproducibility.
[5]	AutoML for Security	AutoML-driven policy tuning	Adaptive model selection improves security	Edge compute demand, data-shift sensitivity	Good step but not feasible for constrained edge systems.
[6]	ML Closed Loops	Assurance loops with AI integration	Clear loop design	Latency, poor inter-domain scaling	Concept sound, but multi-domain deployment unrealistic.
[7]	Cross-Layer Framework	ACROSS orchestration (RAN–cloud)	Demonstrates modular cross-layer orchestration	Scalability unclear; vendor dependence	Proof-of-concept; lacks generalization to heterogeneous domains.
[8]	Fedrated Learning (FL) Security	Aggregation vs. poisoning attacks	Enhances trust in FL	Collusion, high overhead	Secures FL partially, but not scalable for ZSM-wide adoption.
[9]	Lifecycle AI	AI-assisted lifecycle management	Holistic coverage from design to assurance	Operational/tooling complexity	Visionary but hard to operationalize across domains.
[10]	Virtualization in ZSM	NFV/SDN mapped to ZSM	Clarifies MANO–SDN roles	Latency, state consistency issues	Useful mapping but lacks deployment readiness.
[11]	IoT ZTA	Zero-trust enforcement at IoT edge	Lightweight enforcement shown	IoT device constraints	Practical but scalability to IoT swarms doubtful.
[12]	Security Orchestration	Orchestration automation for NGN	Layered tooling view	Cost-effectiveness, maturity untested	Conceptual; economic feasibility questionable.
[13]	Intent-Driven 6G	SLA mapped to intents	Illustrates policy flow from intent	Semantic gaps between domains	Early attempt; needs semantic standardization.
[14]	ZTA Literature	Zero-Trust survey	Consolidates scattered work	Lacks telco/empirical validation	Good overview, but remains theoretical.
[15]	QoE with ML	Hybrid ML for video QoE	Improves user experience	Poor generalization across settings	Narrow use case, not general for ZSM.
[16]	Resource Allocation	Cell-free IoT optimization	Tackles IoT connectivity/orchestration	Weak validation; preprint stage	Interesting but lacks peer-reviewed maturity.
[17]	Smart-City ZSM	Smart highway testbed	Demonstrates vehicular orchestration	Domain-specific, small scale	Real-world demo but not transferable broadly.
[18]	Explainable FL	XAI integrated into FL	Transparency, operator trust	Latency and traffic overhead	Improves trust but adds inefficiency.
[19]	Security Automation	Orchestration of 5G+ security	Coherent building blocks	Complex, tightly coupled	Provides vision, but impractical for dynamic 6G.
[20]	ZSM Evolution	Roadmap to zero-touch	Long-term taxonomy, vision	Legacy migration unsolved	Strategic foresight but lacks actionable deployment path.

TABLE II Critical Analysis of ZSM Research Based on Single Reference

References	Category	Key Attributes	Strengths	Limitations	Critical Insight
[21]	6G Survey	Vision, architecture, requirements	Comprehensive taxonomy of enablers	High-level, lacks ZSM focus	Good baseline for 6G; needs integration with automation testbeds.
[22]	6G AI Use Cases	AI-native (digital twins, XR, automation)	Forward-looking use-case mapping	No empirical validation	Valuable foresight; practical deployments remain future work.
[23]	Network Slicing	Zero-touch slice management survey	Programmable isolation and automation	Assurance and monitoring gaps	Solid foundation; but large-scale resilience still unsolved.
[24]	IoT ZT/ZZ	Zero-trust/zero-knowledge ML for IoT	Unified ML-based IoT security posture	Scalability unclear; preprint only	Interesting concept but weak maturity; lacks peer validation.
[25]	Intent-Based Networking	End-to-end intent/policy enforcement	Vendor-neutral abstractions for interoperability	Semantic mismatches across domains	Strong IBN direction, but real cross-domain harmonization needed.
[26]	AI Privacy in 6G	AI-driven security/privacy frameworks	Anticipates 6G risks, proactive view	No real-world deployment	Conceptual only; must be tested with actual AI workloads.
[27]	Cross-Domain AI	AI requirements for multi-domain orchestration	Highlights coordination/transfer learning needs	API/architecture immaturity	Good problem framing; lacks validation and tools.
[28]	DRL for WLANs	DRL for wireless autotuning	Demonstrates WLAN autonomy benefits	Strong hardware dependence, reproducibility issues	Feasible in lab settings; hard to generalize.
[29]	FL for IDS	Semi-supervised FL intrusion detection	Reduces labels, preserves privacy	High comm. cost; feature engineering overhead	Promising direction but expensive for real-time IDS.
[30]	MLOps for ZSM	QMP platform for ZSM MLOps	Aligns DevOps with MLOps assurance	Edge observability/scalability open	Early integration attempt; requires production evaluation.
[31]	Slice Orchestration	Massive slice orchestration in ZSM	Provides scalable orchestration design	Multi-domain maturity limited	Important for 6G, but interoperability still a bottleneck.
[32]	UAV Edge ZSM	Zero-touch UAV edge management	Supports mobility-aware orchestration	Reliability, energy constraints	Useful for aerial networks but fragile under mobility stress.
[33]	AIaaS (ZT)	AI-as-a-Service with ZSM assurance	Shows AIaaS automation patterns	High deployment costs, governance issues	Interesting model but adoption may be limited by economics.
[34]	XAI and LLMs	Trustworthy ZSM with XAI + LLMs	Improves interpretability	Compute-intensive; safety guardrails needed	Novel combination; but may not be feasible at scale yet.
[35]	Satellite ZSM	AI for non-terrestrial (LEO) networks	Future-proof NTN/LEO focus	Latency, intermittent links	Promising; but NTN ZSM lags far behind terrestrial maturity.
[36]	XAI in 6G	Taxonomy of explainable AI in 6G	Maps interpretable methods across use cases	No benchmarks; still abstract	Good roadmap; field is early-stage and theoretical.
[37]	O-RAN Security	Threats in open RAN	Clear taxonomy of vulnerabilities	Few mitigations; no validation	Strong problem framing; mitigation research urgently needed.
[38]	XAI for Industry 5.0	XAI architecture for Industry 5.0	Human-centric, clear roadmap	Industrial validation missing	Links Industry 5.0 with ZSM/6G; needs pilots to mature.

TABLE III Critical Analysis of ZSM Research Based on Single Reference

References	Category	Key Attributes	Strengths	Limitations	Critical Insight
[39]	Slice Optimization	AI-driven zero-touch slice optimization	Experimental validation at CAMAD'24	Few trials; unclear scalability	Good proof-of-concept, needs large-scale multi-domain trials.
[40]	6G Survey	Broad survey on 6G tech and gaps	Comprehensive taxonomy of enablers	Pre-standardization; weak ZSM/O-RAN focus	Solid reference, but misses automation-centric discussion.
[41]	Resource Allocation	ML-based VNF allocation in 6G	Optimized models for cloud-native VNFs	Synchronization/ coordination overheads	Promising but hard to realize in dynamic edge-cloud.
[42]	IIoT Security	Ensemble learning + ZSM provisioning	Privacy/latency-aware design	Training/compute overhead; lifecycle complexity	Strong design, but costly for IIoT real-time constraints.
[43]	Service Management	AI-enabled CDR analysis for ZSM	Large-scale proactive assurance	Heavy dependence on CDR quality	Effective only in telcos with mature data pipelines.
[44]	Tactile Internet	ZSM frameworks for URLLC	URLLC-focused design	High deployment complexity	Visionary but achieving sub-ms latency remains unrealistic.
[45]	IBN and NTN	Intent-based networking for terrestrial/NTN	Aligns with 5G/6G standards	High inter-domain complexity	Bridges terrestrial–NTN, but integration overhead is huge.
[46]	Green Networks	Net-Zero aligned ZSM design	Connects ZSM with sustainability goals	Depends on policy/regulatory shifts	Important direction but technical maturity is minimal.
[47]	XAI and FL (Slicing)	Turbo-Explainable FL for slicing	Improves FL transparency	Adds pipeline complexity; preprint only	Enhances trust, but validation is limited.
[48]	Neuro-symbolic XAI	Twin-based neuro-symbolic orchestration	Combines symbolic and deep AI for interpretability	High computational cost	Strong academic idea; integration into IoE is challenging.
[49]	Haptics/WCN	Survey on tactile intelligence in 6G	Broad overview of haptic communication	Few real deployments; early stage	Useful vision paper; practical maturity far away.
[50]	Crowd ZSM	Crowdsourcing-assisted ZSM automation	Enhances adaptability via collective input	Security/trust concerns in crowdsourcing	Novel idea but risky for security-critical automation.
[51]	Industrial ZSM	Energy-aware industrial automation	Focus on green deterministic M2M	Only simulation validation	Narrow scope; lacks industrial prototyping.
[52]	Tactile Internet	Intelligent TI requirements for 6G	Clear roadmap linking URLLC and AI	No prototyping; purely conceptual	Sets future direction, but validation missing.
[53]	6G Programme	Hexa-X project insights	Pan-European innovation model	Limited to single flagship consortium	Rich perspective, but biased toward EU approach.
[54]	Microservice Scheduling	DDPG-based VNF scheduling	Improves fairness, reduces starvation	High training cost, scheduling complexity	Good AI-driven attempt; real-time feasibility questionable.

TABLE IV Critical Analysis of ZSM Research Based on Single Reference

References	Category	Key Attributes	Strengths	Limitations	Critical Insight
[55]	Infrastructure Optimization	NFV-based element mgmt. for 5G/6G infra	Improves resource efficiency and life-cycle ops	Operational complexity; multi-domain setup burden	Practical gains but ops overhead may offset benefits at scale.
[56]	6G Evolution	Long-term inventor perspective on mgmt	Strategic vision; highlights trends	Conceptual/subjective; no quantitative eval	Useful horizon scanning; needs empirical grounding.
[57]	Trustworthy AI	XAI/robust AI for 6G resource mgmt	Emphasizes robustness, fairness, transparency	Compute-heavy; scalability in dense nets unclear	Right priorities set; efficiency-aware XAI is missing.
[58]	Organic 6G	Decentralized self-* (config/heal/optimize)	Clear autonomy principles; resiliency goals	No real deployments; mostly theoretical	Inspiring blueprint, but tooling/APIs immature.
[59]	QoS Automation	Zero-touch TSN QoS configuration (AutomAdapt)	Automates TSN flows; reduces manual tuning	Real-time stability and large-scale TSN unproven	Niche but valuable; needs hardware-in-the-loop trials.
[60]	Split FL	Requirements/challenges for split FL in 6G	Better privacy/scalability via partitioning	Wider attack surface; orchestration complexity	Promising for edge; must pair with zero-trust controls.
[61]	Enterprise ZT	Zero-touch invoice processing (ERP)	Demonstrates paperless automation benefits	Narrow scope; not peer-reviewed	Illustrative enterprise case, limited telco relevance.
[62]	Privacy Credentials	Attribute-based credentials for 6G access	Fine-grained identity/privacy control	Legacy integration/adoption barriers	Strong privacy primitive; deployment hinges on standards.
[63]	Neutral Host RAN	NeutRAN: open RAN neutral host for ZSM	Enables RAN sharing; spectrum efficiency	Tenant policy alignment; governance issues	Technically solid; policy/ops agreements are the blocker.
[64]	Privacy Orchestration	Orchestration extended with privacy-by-design	Systematizes privacy across layers	Added complexity; perf. trade-offs likely	Necessary step; needs measurable SLO impact.
[65]	Security Roadmap	Roadmap for secure 6G architectures	Holistic threat/requirement view	Early-stage; limited implementations	Good compass; prioritize actionable controls and metrics.
[66]	User-Centric 6G	Stakeholder-centric 6G survey	Comprehensive ecosystem taxonomy	Very broad; light on deep tech	Helpful context; pair with technical exemplars.
[67]	O-RAN Perspectives	Industry views on open/smart RAN for 6G	Timely industry insight; aligns evolution paths	Strategic only; few technical details	Aligns research with industry needs; requires follow-on specs.
[68]	Distributed Fabric	Unified service-level sensing/compute/comm/control	Holistic 6G service fabric concept	Visionary; lacks prototypes	Strong systems vision; pilot architectures are next.
[69]	Digital Twin (Editorial)	DT–6G interplay editorial	Elevates DT importance for networks	Conceptual; no framework/eval	Sets agenda; actionable DT pipelines still absent.

TABLE V Comparison of ZSM Research Based on Single Reference

References	Category	Key Attributes	Strengths	Limitations
[70]	O-RAN Digital Twin	Digital twin framework for O-RAN evolution toward 6G	Establishes a strong connection between DTs and O-RAN architecture	Implementation and real-time synchronization remain highly complex
[71]	O-RAN Survey (Slicing-Aware)	Comprehensive tutorial/survey of O-RAN with slicing-aware design	Provides holistic taxonomy, clear mapping of RIC layers to KPIs/timescales, and integrates slicing with orchestration and standardization	Survey-level synthesis; lacks empirical benchmarking, XAI integration, and large-scale testbeds
[72]	AI and Energy (Editorial)	Guest editorial on AI and 6G convergence for energy efficiency	Emphasizes sustainability and AI-driven energy optimization in 6G vision	Limited scope as an editorial; lacks technical proposals or case studies
[73]	Slice Management	AI-driven framework for scalable network slice management	Enables large-scale slice orchestration with practical AI-based mechanisms	Integration into heterogeneous networks remains challenging
[74]	Smart Health	Role of 6G in enabling future smart healthcare services	Maps vertical-focused use cases and identifies 6G enablers for healthcare	Domain-limited; broader ZSM implications not covered
[75]	6G Slicing Framework	Proposal of open, intelligent, end-to-end slicing architecture	Presents comprehensive 6G-ready slicing framework with openness and intelligence	Complexity of realization and need for future experimental validation
[76]	Lifecycle AI	REASON approach for lifecycle management of trustworthy AI in 6G	Strong emphasis on AI governance, compliance, and model accountability	Still early-stage; lacks broad real-world testing
[77]	Zero Trust	Survey on Zero Trust Architecture (ZTA) in 6G	Comprehensive review of ZTA applications and challenges for 6G networks	Exploratory survey; limited empirical validation
[78]	6G Survey	Five facets of 6G: architecture, spectrum, AI, security, sustainability	Broad overview of 6G research challenges and opportunities	Very general; limited focus on ZSM implementations
[79]	Cross-Layer Security	Automated cross-layer security for 6G networks	Provides strong integration of automation into security design	Conceptual with limited experimental validation
[80]	XAI and Slicing	Survey on explainable AI for communications and slicing	Enhances transparency and interpretability of AI-driven slicing	Conceptual stage; practical deployment not demonstrated
[81]	AutoRAN	Automated and zero-touch O-RAN system design (AutoRAN)	Practical framework for RAN automation; aligns with O-RAN standardization	Preprint work; untested in real deployments
[82]	Drift Detection	Dual self-attention mechanism for drift detection in 6G	Novel ML-based approach for robust drift management	Computationally complex; performance-cost tradeoffs
[83]	SatCom AI	Survey on AI applications in satellite communications	Offers comprehensive taxonomy across SatCom domains	Broad scope; limited ZSM-specific depth
[84]	5G IIoT Testbeds	Review of testbeds for industrial IoT	Practical evaluation of IIoT testbeds and lessons learned	Primarily 5G-focused; limited extension to 6G
[85]	IoT Security	Cross-layer secure and low-latency communication in IoT	Strong analysis of latency-security trade-offs in IoT	Domain-limited; not fully generalized to 6G ZSM

TABLE VI Comparison of ZSM Research Based on Single Reference

References	Category	Key Attributes	Strengths	Limitations
[86]	XAI in O-RAN	Tutorial and survey of explainable AI in 6G O-RAN	Detailed taxonomy, use cases, and challenges for XAI in O-RAN	Complexity of implementation; many open research directions
[87]	LLM Security	Position paper on LLMs in 6G security	Identifies novel opportunities for LLM-based security in 6G	Early-stage, speculative with no implementations
[88]	FL Cybersecurity	Survey of federated learning for cybersecurity	Strengthens privacy and trust through collaborative learning	High communication and computation overhead
[89]	LLMs for Management	Survey of LLM applications in communication and service management	Wide insights into LLM integration for networks and management	Challenges in scalability, governance, and reliability remain
[90]	AI in 6G	Survey on AI concepts, techniques, and standards for 6G	Well-structured overview linking AI methods to 6G standardization	Generic treatment; limited ZSM depth
[91]	Vertical Services	Future of vertical services in 6G	Provides clear innovations for vertical-specific 6G applications	Conceptual proposals; requires validation in testbeds
[92]	Intent and LLMs	Extending intent-based management with language models	Introduces innovative LM-driven intent handling in B5G infrastructures	Early-stage; demonstrated only at conceptual/demo level
[93]	AI Forecasting	Attention-driven AI model generalization for workload prediction	Strong focus on AI-driven generalization across heterogeneous workloads	Needs validation in real-world 6G deployments
[94]	Edge-Cloud Orchestration	AERO: Sub-1K-parameter lightweight forecasting model	Highly efficient, low-complexity design, scalable across edge-cloud	Limited integration with security and lifecycle orchestration
[95]	Cloud-Edge AI Trends	Forecasting trends using attention mechanisms in cloud-edge computing	Provides visionary insights on AI–cloud-edge convergence	Mostly conceptual, limited experimental validation
[96]	Dynamic Slicing	ML-driven reconfiguration for 5G/6G virtualized slices	Demonstrates practical slice reallocation and forecasting	Complex orchestration in multi-domain heterogeneous networks
[97]	Agentic AI	AgentEdge for service orchestration in edge-cloud continuum	Introduces novel paradigm of agentic AI for orchestration	Preprint stage; lacks empirical and large-scale validation
[98]	Agentic AI Networking	Foundation model-as-agent approach for 6G networking	Integrates generative models with agentic reasoning for goal-driven orchestration	Early-stage; lacks benchmarks and system-level trials
[99]	Edge Agentic AI	Framework for autonomous optimisation in O-RAN using agentic AI	Multi-agent adaptability for edge and RAN optimization	Limited scalability analysis; simulation-focused
[100]	AgentRAN Architecture	Hierarchical agentic AI for autonomous control of Open 6G RANs	Provides intent-to-action orchestration with layered autonomy	Preprint; no validation in real-world O-RAN testbeds
[101]	Agentic Marketplace	Agoran: Open marketplace for 6G RAN automation	Novel agent-based stakeholder negotiation and service deployment	Governance, standardization, and trust mechanisms underdeveloped

TABLE VII Comparison of ZSM/6G Research Based on Single Reference

References	Category	Key Attributes	Strengths	Limitations
[102]	Agentic Observability	MX-AI: Observability and control for Open and AI-RAN	LLM-powered agents enable transparency and real-time orchestration	Early-stage framework; explainability and safety concerns remain
[103]	Agentic Core Networks	Mission-oriented, AI-empowered mobile core network	Aligns orchestration with mission-critical KPIs; autonomy-focused	Prototype-level; lacks evaluation in full-scale 6G scenarios
[104]	Reliability of GenAI in 6G	Enhancing generative AI reliability with agentic workflows at the edge	Tackles hallucination and reliability issues of GenAI in 6G	Conceptual; requires integration with operational 6G platforms
[105]	AI-Native Architecture	Task-driven design approach for 6G AI-native systems	Provides systematic integration of AI into core network architecture	Early conceptual stage; requires testbed validation
[106]	AI Architectures	Advanced architectures integrating agentic AI for wireless networks	Bridges agentic AI with system-level architectural innovations	Preprint; lacks deployment metrics and empirical benchmarks
[107]	Edge General Intelligence	Agentic AI and agentification for edge intelligence in 6G	Comprehensive vision of edge general intelligence with agents	Broad and conceptual; lacks technical depth on orchestration pipelines
[108]	Maturity Models	Agentic AI maturity model for 6G software ecosystems	Provides layered adoption model for industrial readiness	More business-oriented; limited focus on technical ZSM challenges
[109]	Security Survey	Multi-layer survey of 6G security (physical, connection, service)	Provides holistic taxonomy across three layers of 6G	Limited focus on orchestration and ZSM-specific aspects
[110]	Architectural Survey	Survey of architectural approaches for 6G networks	Highlights modular, sustainable, and AI-native design trends	General overview; lacks detailed ZSM orchestration insights
[111]	Challenges Survey	Comprehensive survey of challenges in 6G networks	Identifies open issues in scalability, latency, and orchestration	Lacks in-depth treatment of AI-driven ZSM solutions
[112]	Orchestration Survey	Network service orchestration survey	Provides foundational understanding of orchestration frameworks	Pre-6G; focuses on NFV/SDN, not AI-native ZSM
[113]	LLM Agents for 6G Orchestration	Proposes LLM-based agentic orchestration for physical-layer task automation	Introduces AI-native orchestration paradigm using LLM agents	Early-stage; conceptual with limited deployment validation
[114]	Autonomous Network Management for 6G Communication	Comprehensive survey of frameworks and challenges in autonomous 6G network management	Synthesizes state-of-the-art architectures, AI-driven orchestration, and security into one structured review	Broad coverage; still conceptual with few real-world testbeds
[115]	Next-Generation 6G Network Management with OSS-GPT	Introduces GPT-powered OSS for 6G orchestration and service management	Proposes LLM-based automation at the MANO layer to improve scalability and adaptability	Early demonstration; limited to proof-of-concept scenarios
[116]	6G Simulators Survey	Systematic review and comparison of existing 6G simulators	Covers integration of AI, digital twins, and orchestration into simulation platforms	Lacks validation across diverse industrial deployments

TABLE VIII Comparison of ZSM/6G Research Based on Single Reference

References	Category	Key Attributes	Strengths	Limitations
[117]	O-RAN Security Survey	Explores intelligent control in 6G O-RAN; highlights risks vs. opportunities	Provides comprehensive survey of attack surfaces and mitigations for RIC-based orchestration	Early-stage; mostly conceptual, limited deployment validation
[118]	O-RAN Security Testing	Empirical testing of Near-RT RIC and A1 interface using μONOS/OSC	Offers hands-on evaluation of RIC vulnerabilities, showing practical risks in open-source O-RAN implementations	Focused only on μONOS and OSC; may not generalize across all vendor implementations
[119]	O-RAN Security Framework	Layered threat model and defense strategies for intelligent O-RAN	Provides structured perspective bridging AI orchestration with layered security defenses	Conceptual model; requires real-world validation and integration with standardization bodies
[120]	Security Survey	Broad survey on 5G–6G security, privacy, and standardization pathways	Provides high-level synthesis of risks, mitigations, and alignment with evolving standards	Conceptual scope; lacks detailed empirical validation or domain-specific case studies
[121]	Privacy-Preserving AI Framework	DP-FL framework for 6G-enabled consumer electronics	Demonstrates integration of federated learning with differential privacy for securing personal/IoT devices	Limited scalability analysis for large-scale telecom environments; mostly focused on consumer use cases
[122]	Explainable AI in 6G O-RAN (Survey)	Tutorial and survey on integrating XAI into O-RAN for interpretability, trust, and automation	Provides systematic taxonomy of XAI methods, use cases, and challenges in 6G O-RAN	Conceptual; lacks large-scale deployment and empirical benchmarks
[123]	Digital Twin for O-RAN	Introduces digital twins to model, simulate, and optimize O-RAN performance	Demonstrates proactive fault management, predictive optimization, and real-time monitoring	Limited scalability; synchronization and interoperability issues remain
[124]	Intelligent O-RAN for B5G/6G	AI/ML-enabled RAN; non-RT/near-RT RIC with xApps/rApps; control loops & telemetry	Maps ML to RIC timescales; KPIs & standards hooks; concrete use cases	No large-scale trials/benchmarks; security/XAI only briefly noted
[125]	O-RAN & 6G Vision (Preprint)	Conceptual role of O-RAN as 6G enabler; openness/programmability	Highlights challenges, trade-offs, and research roadmap	Speculative; minimal empirical validation
[126]	Open RAN Trends Survey	Broad review of O-RAN developments, deployments, and policy aspects	Offers taxonomy of architectures, AI-enabled RIC functions, and regulatory considerations	Survey scope broad; less technical detail on specific algorithms or implementations
[127]	Guest Editorial (JSAC)	Editorial framing O-RAN as a new paradigm for cellular networks	Highlights openness, programmability, and AI as enablers of future intelligent networks	Overview only; not a technical contribution, serves as contextual framing
[128]	Resource Allocation in O-RAN	Proposes probabilistic forecasting for cloud-native O-RAN resource allocation	Improves latency, throughput, and energy efficiency under variable traffic loads	Focused on simulation results; real-world deployment and scalability untested

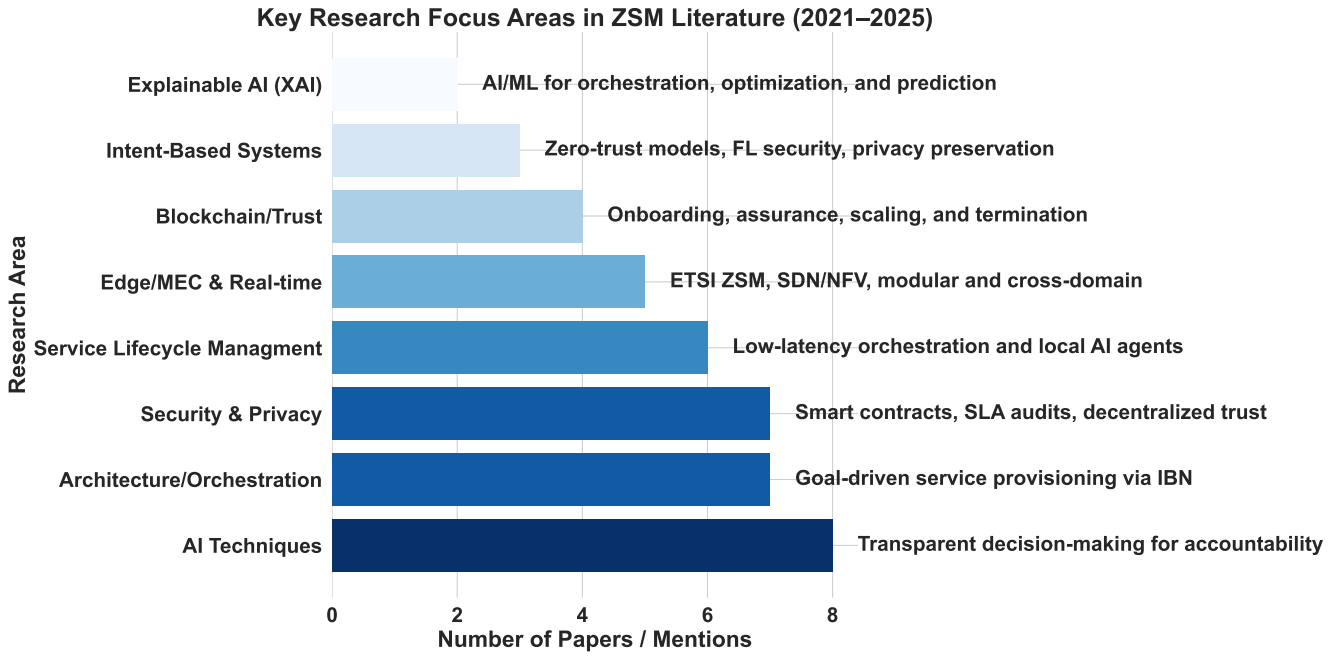

Fig. 3: Focus areas in ZSM across architecture, AI/automation, security, lifecycle, and future enablers.

TABLE IX Feature Comparison of ZSM Research (Part 1: Architectural and Automation Attributes, extended with Agentic AI)

References	Category / Method	Modular Arch.	AI / ML	Blockchain	Cloud-Native	Federated Learning	Reinforcemet Learning	Intent-Based	Multi-Domain	Agentic AI / LLMs
[1], [4]	ZSM Frameworks	Y	Y	N	Y	N	N	Y	Y	N
[5], [6]	AI-Powered Automation	N	Y	N	P	Y	Y	N	Y	N
[8], [60]	Federated	N	Y	N	N	Y	Y	N	N	N
[2], [19], [64]	Security / Zero Trust / IoT	N	Y	N	P	Y	N	N	Y	N
[34], [47]	Cloud-Native , Blockchain and XAI	Y	Y	Y	Y	P	N	Y	Y	N
[31], [44]	Intent-Based	Y	Y	N	Y	N	N	Y	Y	N
[66]	Survey / Overview	N	Y	N	N	N	N	N	N	N
[41]	QoE / Resource Management	N	Y	N	P	N	Y	N	Y	N
[48]	Smart City / Explainable AI	N	Y	N	P	N	N	N	N	N
[50], [56]	Cross Domain Deployment	Y	Y	N	Y	N	Y	Y	Y	N

Y = Yes (high focus), P = Partly (partial focus), N = Not covered, XAI= Explainable Artificial Intelligence, FL= Federated Learning, ML= Machine Learning, LLM = Large Language Model

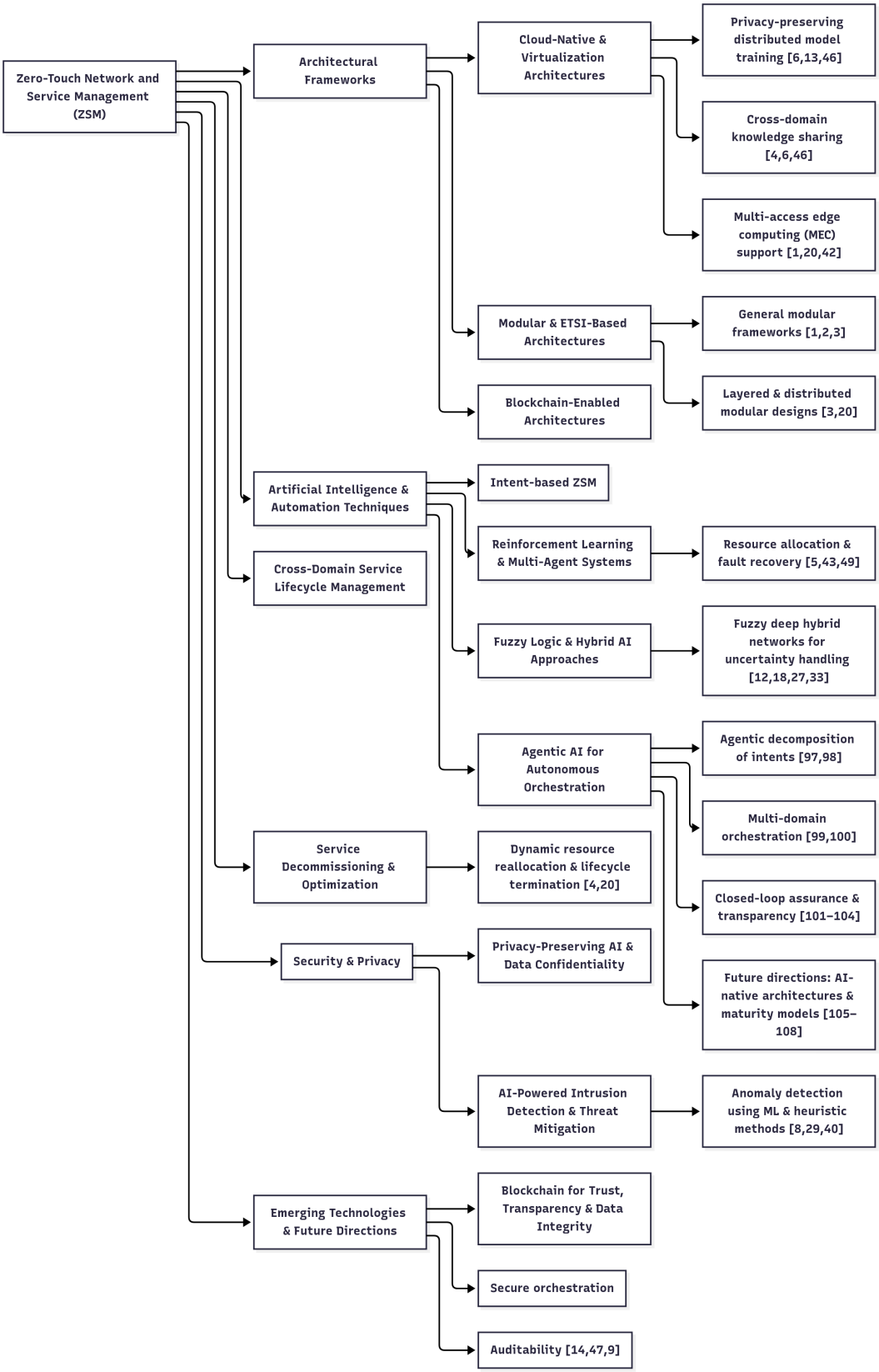

Fig. 4: Taxonomy of Zero-Touch Network and Service Management (ZSM).

TABLE X Feature Comparison of ZSM Research (Part 2: Security, Lifecycle, Edge, Analytics and Agentic AI)

References	Category / Method	Lifecycle Automation	Security	Privacy	6G / Aerial	Explainable AI	Edge / MEC	Real-Time Analytics	Agentic AI / LLMs
[1], [4]	**ZSM Lifecycle Orchestration**	**Y**	**Y**	**P**	**Y**	**N**	**Y**	**Y**	**N**
[5], [6]	**Fault Mgmt / Closed Loop AI**	**Y**	**Y**	**Y**	**P**	**Y**	**Y**	**Y**	**N**
[2], [11], [14]	**Security / Blockchain / Zero Trust**	**N**	**Y**	**Y**	**N**	**N**	**P**	**N**	**N**
[24], [60]	**Federated AI / IoT Security**	**N**	**Y**	**Y**	**P**	**P**	**N**	**Y**	**N**
[19], [41]	**QoE / Resource Mgmt / IoT**	**Y**	**Y**	**P**	**Y**	**N**	**Y**	**Y**	**N**
[25], [50]	**Intent Based Systems**	**Y**	**P**	**N**	**Y**	**N**	**Y**	**Y**	**N**
[23], [66]	**Surveys and Vision Papers**	**P**	**N**	**N**	**Y**	**P**	**N**	**P**	**N**
[48], [57]	**Smart City / Explainable AI**	**Y**	**Y**	**N**	**P**	**Y**	**P**	**P**	**N**
[27], [56]	**MLOps/ Cross Domain**	**Y**	**Y**	**P**	**Y**	**P**	**Y**	**Y**	**N**
Y = Yes (high focus), P = Partly (partial focus), N = Not covered, MLops = Machine Learning Operations, IoT = Internet of things									

A. *ZSM Architectural Frameworks (RQ1)*

Architecture-centric contributions appear in Table I in refrence [20] and are complemented by forward looking vertical items across Tables II–IV [63], [68]. Read these alongside Fig. 7, which visualizes the modular and ETSI based views referenced under Key Attributes.

ZSM architectures must accommodate rising heterogeneity, elastic scaling, and intelligent automation across access–edge–core and multi-domain fabrics.Cloud-native, modular designs aligned with SDN / NVF remain fundamental, while recent surveys emphasize a shift toward AI-native architectures that elevate intelligence to a first-class network function [110], [114]. Open and programmable RAN stacks further externalize controled analytics into non-RT or near-RT planes, preparing the ground for closed-loop autonomy [67], [124].

Microservices and cloud-native orchestration:

Concrete systems adopt microservices to decouple control, assurance, and data planes. Architecture in [41] optimizes resource allocation for microservices-based VNFs in 6G, [54] introduces DDPG-driven dynamic prioritization to mitigate starvation in service deployments, and [55] proposes an NFV element management system that improves lifecycle efficiency. As summarized in Tables, these designs consistently score well on elasticity and modularity but introduce training and coordination overheads and operational complexity.

Centralized vs. distributed control:

[20] outlines a hierarchical AI-driven orchestration path that cleanly maps intents to assurance, yet risks control bottlenecks in multi-operator contexts. Conversely, [31] (massive slicing) advocate more distributed, self-organizing control that boosts local responsiveness at the cost of weaker global optimality. A unifying, service-level fabric that merges sensing, computing, communication, and control is proposed in [68], offering a holistic architectural direction but still lacking prototypes at scale.

E2E slicing and domain federation:

Architectural blueprints for open, intelligent and end-to-end slicing in 6G [75] and neutral host RAN sharing [63] illustrate how domain federation can be realized with clear API boundaries and standardized control loops. Digital twins for O-RAN [70] extend this stack with safe policy testing and what-if analysis, yet introduce synchronization and integration complexity.

Maturity and validation gaps:

Across Parts I–IV, the Strengths columns consistently highlight modularity, openness, and AI-alignment and the Limitations converge on reproducibility, multi-domain interoperability, and real-world validation at scale. Empirical studies exist but are narrow in scope [4], while programmatic viewpoints e.g., Hexa-X, [53] provide valuable process insight with limited generalizability.

Transparency and accountability are also emerging drivers. [34], [38] highlight the role of XAI in explainable orchestration, enabling user-centric auditing and improving operator trust Tables II–V. However, these remain at prototype or survey stage and do not yet mitigate semantic drift in multi-vendor intents. [25] frames intent-based networking as a unifying abstraction, while [24] advances this with adaptive intent to policy mappings for IoT, but evaluations

TABLE XI Comparative Analysis of Prior ZSM Surveys vs. This Work

References	Survey Focus	AI/ML	Security	Lifecycle	Intent	Agentic AI / LLMs	Key Gap Filled by Our Work
[1]	Network automation (5G/6G)	H	L	L	L	L	Unified taxonomy (AI, lifecycle, security, intent)
[6]	ML-assisted closed loops	H	L	L	L	L	Generalizes multi-domain, agentic AI and lifecycle
[8]	FL security in ZSM	L	H	L	L	L	Bridges FL security with orchestration and reproducibility
[10]	Virtualization	L	L	L	L	L	Adds benchmarking and comparative evaluation
[13]	Intent-driven systems	L	L	L	H	L	Extends intent into AI-native orchestration
[23]	Slicing survey	L	L	M	L	L	Embeds slicing within lifecycle taxonomy
[31]	Slice M&O in 6G	L	L	M	L	L	Extends lifecycle to scaling, optimization, assurance
[33]	AI-as-a-Service	H	L	L	L	L	Adds reproducibility and benchmarking
[86]	XAI in O-RAN	H	L	L	L	L	Generalizes XAI across lifecycle, security and intent
[109]	6G Security	L	H	L	L	L	Unifies security with orchestration and AI/ML
[110]	6G Architectures	M	L	L	L	L	Adds automation taxonomy and agentic AI orchestration
[111]	6G Challenges	M	L	L	L	L	Provides comparative eval and reproducibility roadmap
[112]	Orchestration (pre-6G)	M	L	L	L	L	Evolves orchestration into AI-native and agentic contexts
This Work	**ZSM Roadmap (6G)**	**H**	**H**	**H**	**H**	**H**	**First integrated taxonomy (AI, security, lifecycle, intent, agentic AI)**

H = High Coverage, M = Moderate Coverage, L = Low Coverage

TABLE XII Essential technological features for autonomous network operation mapped to foundational research (Part A: Core features).

References	Feature Category	Included Features
[1], [31]	Architecture (ZSM/O-RAN & Slicing)	Modular ETSI/NFV/SDN design; open/neutral-host RAN; end-to-end slice management; organic/adaptive architectures; cross-layer/domain composition
[4]	Zero-Touch Orchestration (Practice)	Experimental ZTM orchestration and operations
[6]	ML-Assisted Closed Loops	Machine-learning–assisted closed-control loops for ZT networks
[3], [28]	DRL for Zero-Touch Networks	DRL (incl. federated/zero-touch DRL) for WLAN/O-RAN orchestration
[47], [60]	Federated / Split Learning for 6G	Split/federated learning for constrained 6G settings; FL with explainability for trustworthy slicing
[5]	AutoML-in-the-Loop	AutoML use-cases enabling zero-touch network/security analytics and assurance
[47]	TEFL for Trustworthy Slicing	Turbo explainable federated learning to improve slice trust and transparency
[2], [77]	Zero-Trust Patterns	Zero-trust reference architectures and controls for 5G/6G
[37]	O-RAN Threat Model	Security challenges and opportunities for Open RAN
[79]	Cross-Layer Automated Security	Cross-layer automation for 6G security
[11], [85]	Secure / Low-Latency IoT	Industrial/edge IoT security with latency constraints
[87]	LLMs in 6G Security	Challenges and opportunities of LLMs for 6G security
[62]	Privacy Credentials	Attribute-based credentials (privacy-preserving)
[64]	Privacy-Aware Orchestration	Orchestration extensions for privacy
[60]	Privacy-Preserving ML	Federated/split learning for data minimization
[24]	IoT Privacy Enablement (Zero-Trust)	Privacy-aware IoT security enablement
[9], [30]	Service Lifecycle & Assurance	AI-assisted service lifecycle (onboarding→assurance→decommission); MLOps pipelines for assurance
[71]	Operational Security (During Operations)	Federated-learning–based intrusion detection integrated into zero-touch operations
[76]	Trustworthy AI Model Lifecycle	Model onboarding, monitoring, drift detection, governance and retirement for 6G networks
[32], [33]	Edge / MEC (incl. UAV)	UAV/vehicular edge management; pervasive AI-as-a-Service at the edge
[35]	Satellite / NTN Integration	Zero-touch management for satellite/NTN use cases
[42]	IIoT Provisioning	Adaptive multi-resource provisioning and security for IIoT
[44], [52]	Tactile Internet Support	Ultra-low-latency/reliability requirements and enablers for tactile services

TABLE XIII Essential technological features for autonomous network operation mapped to foundational research (Part B: Intent, Agentic AI, and Surveys).

References	Feature Category	Included Features
[13], [25], [45]	Intent-Based Systems (Classical IBN)	Goal-oriented intent parsing; policy abstraction; IBN for zero-touch service automation
[92]	LM-Augmented Intent Pipelines	LLM-assisted intent extraction/validation; intent-to-policy compilation with LM support
[25], [31], [50]	Intent-Driven Automation	Automated policy enforcement/self-configuration; adaptive SLA assurance via closed loops and MLOps
[69], [70]	Digital Twins for O-RAN	Digital-twin what-if testing and validation; safe rollout/rollback support
[24], [62], [64]	Blockchain-Backed Control (Selective)	Smart-contract style trust/immutability; secure orchestration/ledgering (when appropriate to ZT/IoT frameworks)
[7], [63], [75]	Multi-Domain / Cross-Domain Operation	Cross-layer provisioning for verticals; neutral-host/federation; scalable slice management across domains; open, intelligent E2E frameworks
[57], [80], [86]	Explainable/ Trustworthy AI	XAI/LLMs for operator trust; robust/explainable RM for 6G; tutorials/surveys on XAI in (O-)RAN and slicing; survey of XAI for 6G comms
[5], [20], [59]	Real-Time Analytics & Assurance	Telemetry-driven prediction; security AutoML use cases; resource/traffic analytics for closed-loop control; CDR-driven service management; zero-touch QoS flow tuning
[97], [99]	Agentic AI for Orchestration	Foundation-model–as-agent approaches; multi-agent orchestration in edge/cloud; agentification for O-RAN optimization
[100], [102]	Agentic AI Architectures	AgentRAN hierarchical orchestration; Agoran open marketplace; MX-AI observability platform for AI-RAN
[103], [108]	Reliability & Maturity Models	Mission-oriented agentic AI core networks; reliability of GenAI at edge; layered maturity models for agentic ecosystems
[109], [112]	Survey Insights	Multi-layer 6G security surveys; architectural surveys; orchestration surveys; comprehensive challenge taxonomies for ZSM and 6G

show inconsistencies across service types echoing semantic ambiguity reported in broader surveys [109], [112]. Integration with foundation models is further explored in [115], which demonstrates GPT powered OSS modules for service management, but adoption remains limited by legacy OSS/BSS coupling.

Observed limitations (RQ1):

From the Limitations columns in Tables I–VIII and confirmed by surveys [109], [111]:

- Persistent semantic ambiguity in intents across vendors and domains,
- Scarcity of multi-domain, multi-operator validations (most prototypes remain single-domain),
- Migration friction for legacy OSS/BSS and lack of standardized APIs for cross-vendor orchestration, and
- Absence of reproducible, large-scale testbeds validating AI-native RAN and organic network concepts.

These gaps motivate our roadmap in RQ5 and justify the ontology/validation agenda introduced later.

*1) **ZSM Architectural Overview***

The ZSM architectural framework is designed to enable autonomous network and service management across heterogeneous and multi-domain environments. It directly addresses the complexity of 5G/6G ecosystems, where IoT proliferation, edge cloud convergence, and ultra-low latency applications require advanced automation. Core objectives

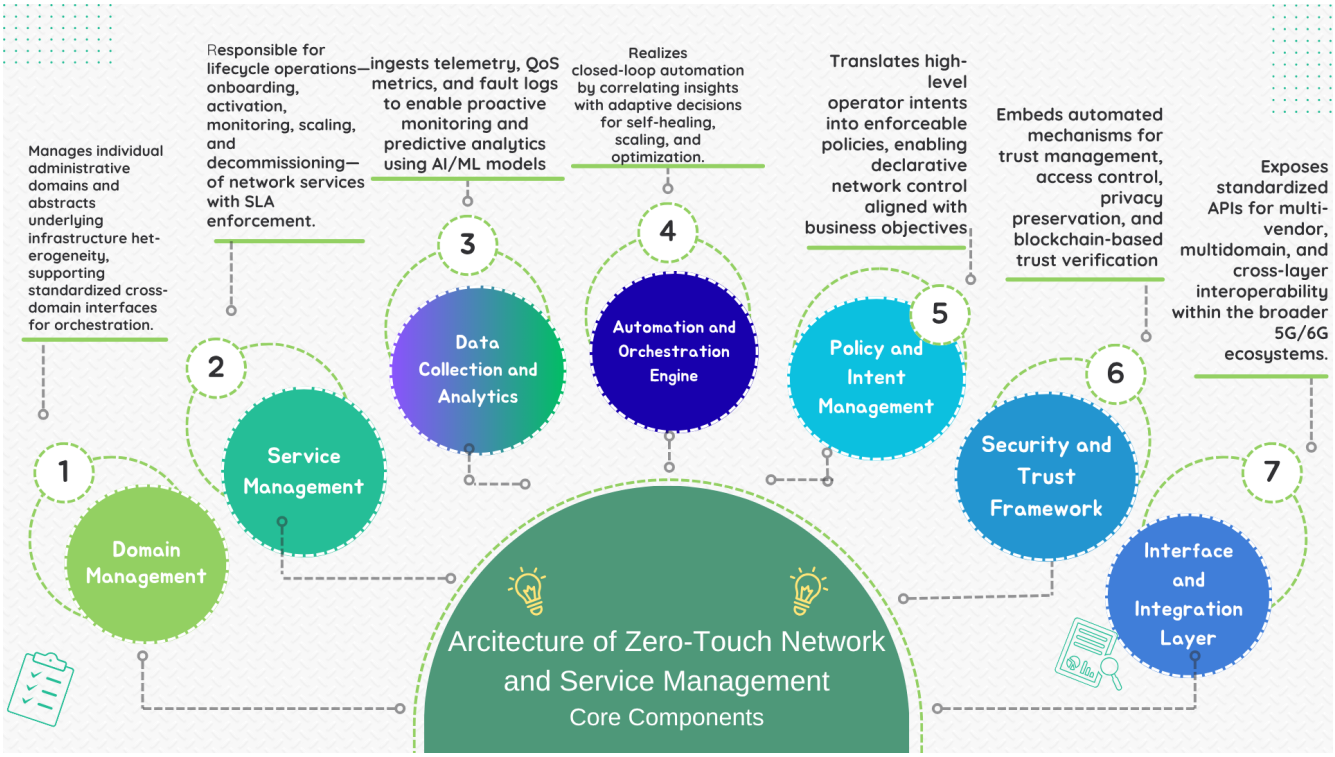

Fig. 5: Core components of ZSM: functional blocks that interact to create a self-managing, self-optimizing, and autonomous network system according to ETSI standards.

include proactive service assurance, closed-loop orchestration, and fault management with minimal human intervention for offloading operational burdens from network operators. In line with the ETSI ZSM reference model, these frameworks envision communication systems that are self-scaling, self-securing, and self-optimizing, tightly coupled with AI-driven analytics [20], [21], [110].

The modular view is illustrated in Fig. 5, which highlights the essential functional blocks and their interactions for building self-managing systems. This structure is also reflected in recent proposals for distributed fabrics [68], O-RAN evolution [70], and open/intelligent slicing frameworks [75].

2) Core Components

The architecture of ZSM consists of the following pivotal elements:

- **Domain Management:** Administrative domains (access, transport, core, verticals) are managed by standardizing the orchestration interfaces and ensuring end-to-end coordination [31].
- **Service Management:** Manages the service lifecycle which includes onboarding, activation, monitoring, elastic scaling, decommissioning, and SLA and QoE enforcement [23].
- **Data and Analytics Fabric:** Consolidates telemetry and KPIs and fault logs for predictive analytics, anomaly detection, and AI-driven forecasting [9], [42].
- **Automation and Orchestration Engine:** Real-time analytics are coupled with adaptive reconfiguration actions to achieve closed-loop automation [6], [20].
- **Policy and Intent Management:** Operator intents are transformed into executable policies across layers and domains, closing semantic gaps in intent-based networking [24], [25].
- **Security and Trust Management:** Trust evaluation, zero-trust enforcement, access control, and privacy-preserving methods (e.g., FL and blockchain) are integrated [2], [62].
- **Integration and Interface Layer:** Service-based APIs are provided for cross-domain federation, vendor neutrality, and OSS/BSS alignment [112], [115].

Paragraphs can be provided in separate boxes. Every person has their different writing style. The above provided seems more technical than necessary and thus i aimed for a simpler version.

3) Design Principles

The ZSM frameworks of toady continue to evolve and build on the foundational design principles set of the ETIS and their newly created open standards.

- **Modular and Service Based Interface (SBI):** The service-oriented components are modular and loosely coupled offering a highly scalable and easy to implement configuration [18], [110].
- **Distributed and Hierarchical Control:** The decision of the local "edge" and the global commander is a trade off of latency and consistency [19], [31].

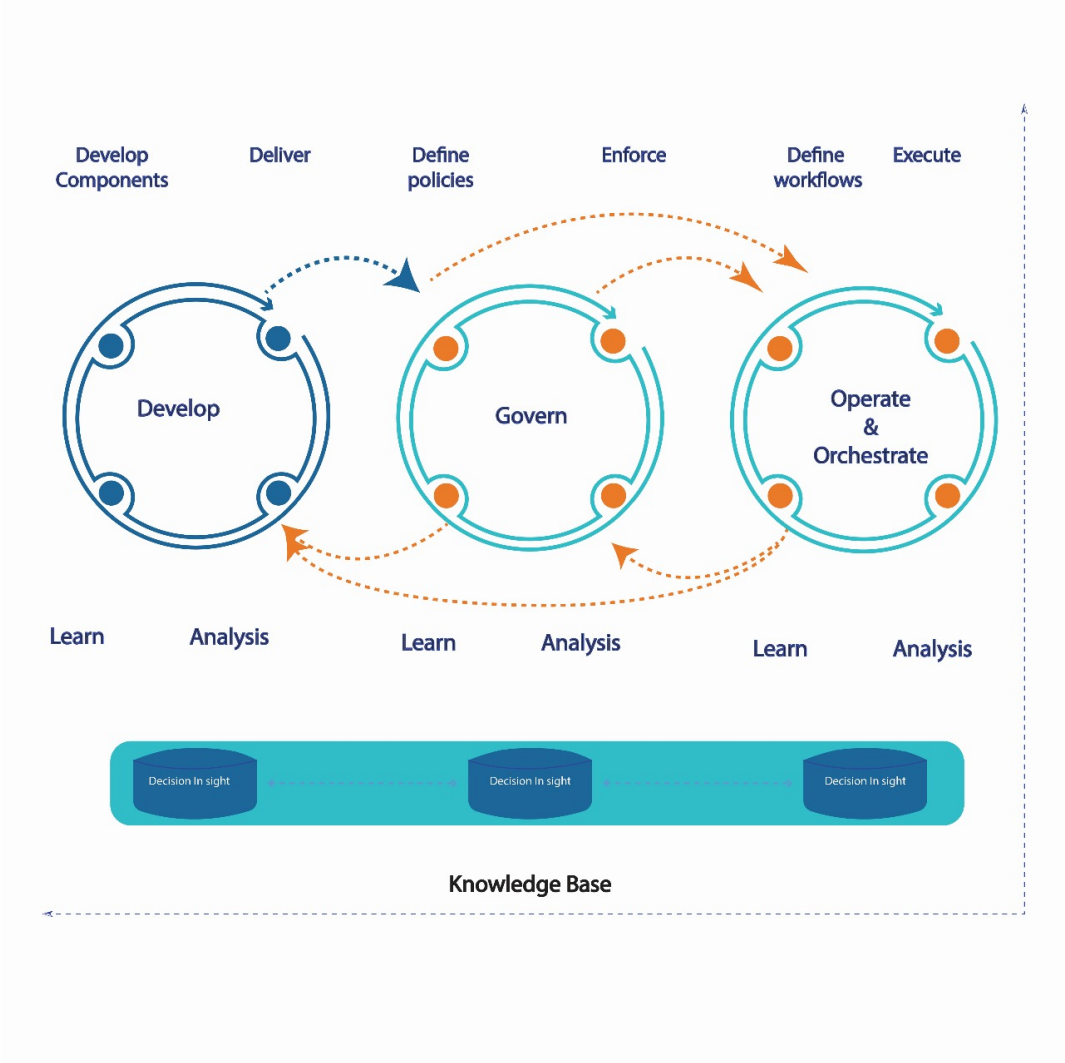

Fig. 6: Core functional cycles of Zero-Touch Management: continuous development, learning, and knowledge orchestration.

- **Closed Loop Automation:** The ability to self configure, heal, and optimize in a continuous manner is accomplished through the observe, analyze, decide, act (OADA) cycle [6], [20].
- **AI-Driven Fault Prediction:** The capacity to predict defects, plan the intent, manage the resources, and translate the intent is accomplished through the use of AI and Machine Learning [9], [113].
- **Multi-Domain and Cross-Domain Orchestration:** The ability to operate through the different domains of technology, different domains of the same structure, and different operator domains [25], [112].
- **Privacy and Security by Design:** The use of Zero-Trust and Privacy Protecting Mechanisms (Federated Learning, BlockChain, and Attribute Based Credentials) [2], [62].
- **Open and Interoperable:** Is aligned with the O-RAN and ETIS ZSM frameworks using open standards to lessen vendor lock and with the open APIs [67], [126].
- **Intent Based Management:** Works on bridging the human aspirations and the machine through enforcement of the policy which is translated to semantic level [24], [115].
- **Knowledge-Driven Operations:** Constructs learning systems using historical data as well as knowledge graphs to predict anomalies and used for optimization [42], [111].

4) Key Enablers of ZSM

ZSM architectural frameworks form the foundation for zero-touch network and service management, enabling smart automation and scalable control across dynamic network landscapes. With the transition from 5G to 6G, networks demand AI-native orchestration, federated trust, intent-driven service provisioning, and multi-domain integration. Key paradigms include ETSI modular standards, cloud-native orchestration, blockchain-based trust frameworks, and infrastructures that integrate terrestrial, aerial, and satellite nodes.

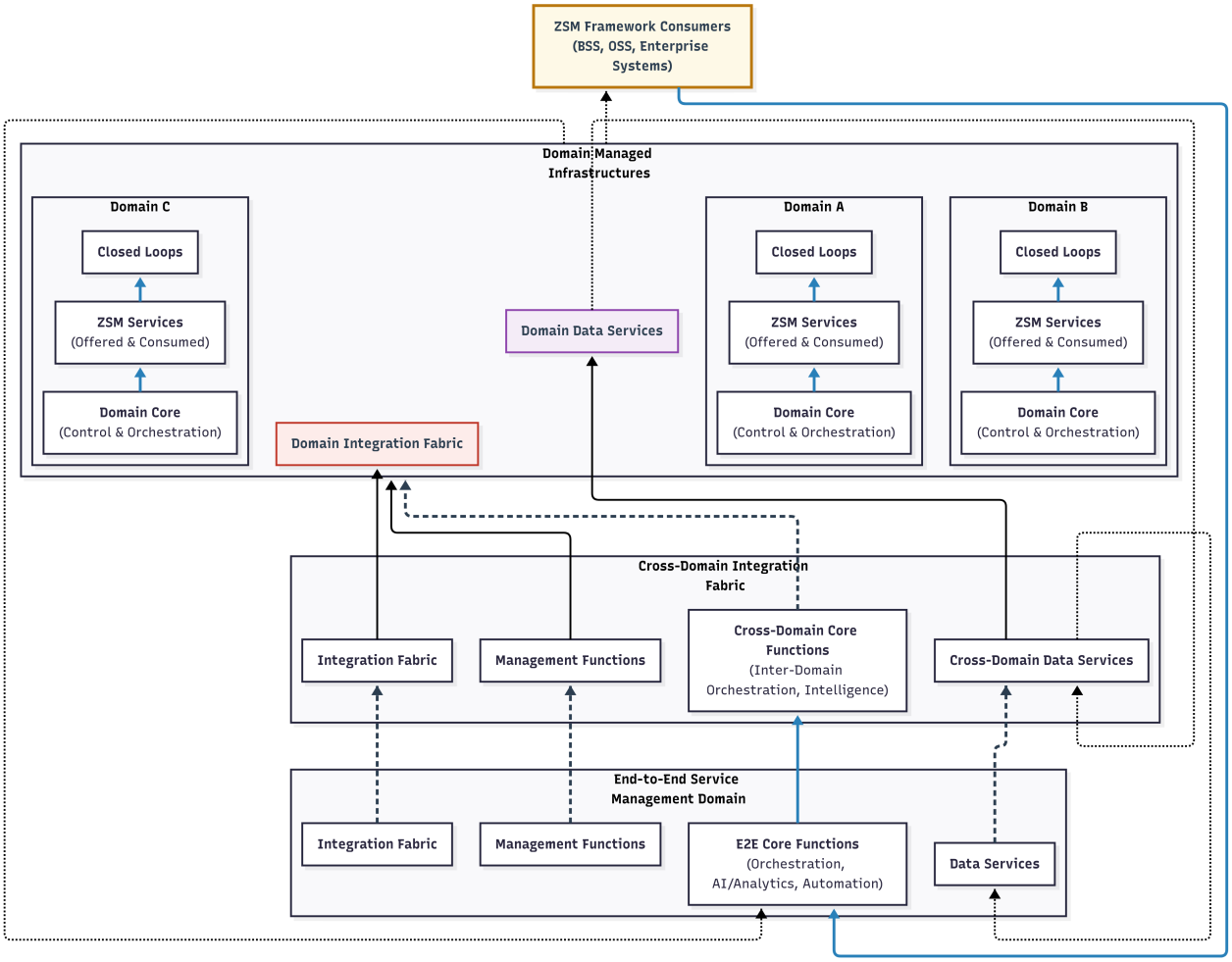

Fig. 7: Modular and ETSI-based architectures for Zero-touch Service Management (ZSM). Functional blocks are organized into core, management, data, and integration fabrics. These blocks can be flexibly composed across domains, ensuring interoperability, scalability, and AI-driven assurance. The ETSI view emphasizes service-based interfaces, closed-loop automation, and cross-domain orchestration as foundations for self-managing 5G/6G ecosystems.

Modular and ETSI Architectures

The system illustrated in Fig. 7 within ETSI Based and Modular architechtures can be separated into functional blocks with loose coupling: core, integration, management, data, and domains, which communicate with each other through standard interface constructs. This modularity permits deployment without concern for vendor, agility in upgrades, and interoperability in heterogeneous 5G/6G conditions. Each BSS/OSS and enterprise system in conjunction with the orchestration layer sends/receives intent, making them to operator actions. These operator actions have recently been reinforced intent based modular frameworks which have come to be called their name [24], [25], [115].

The main architectural developments include the following:

- **Closed Loop Automation (CLA):** Integrating self governing observe–analyze–decide–act (OADA) cycles for diagnostics, assurance, and self-healing.
- **Federated Domain Orchestration:** Enabling cross telco, enterprise and vertical slices interoperability through model driven APIs (e.g. TOSCA, YANG).
- **AI Enabled Analytics Modules:** Delivering real-time forecasting, SLA breach anomaly detection, and SLA breach root cause analysis for SLA compliance guarantees.

The newest adaptations of ETSI compliant frameworks incorporate digital twins for validating policies safely [70], [123], enabling testing, fault forecasting, and optimization prior to actual deployment. Such frameworks enhance the orchestration and execution validation risk mitigation by testing results in a simulation environment. Within the same timeframe, the architecture have become more focused on specific use cases for 6G, such as time sensitive networking [59], multipath service chains, and cross terrain, aerial and non terrestrial network [35], [45] cross domain orchestration. These activities expand the foundational ETSI-ZSM reference model into diverse, multi ecosystem, layered systems.

Cloud Native and Virtualization Architectures

The ZSM microservice driven scaling, rapid service deployment, and the use of the cloud are now inseparably intertwined. Studies [10], [18] explains the orchestration of Kubernetes with respect to geo-distributed ZSM environments, highlighting how function instantiation, CI/CD pipelines, and containerized service meshes are implemented. This microservice model, in turn, enables the agility, reusability, and vendor lock-in avoidance.

Technologies such as network functions virtualization and software defined networking add complementary layers of abstraction over compute, storage, and network resources elasticity for on demand elasticity, automated lifecycle control, and simplicity of operations. Efficiently tuned service chains and dynamically provisioned slices of the network are better aligned to the resource use, within the constraints of the QoS.

Multi access Edge Computing (MEC) extends this paradigm by relocating compute and storage to the network edge, enabling:

- Low-latency applications such as XR and autonomous driving.
- Edge-based inferencing and policy enforcement with distributed AI.
- Delegation of control from central orchestrators, reducing signaling overhead.

Finally, distributed orchestration engines have begun to be integrated into the control fabric of the cloud to autonomously carry out operational intents, handle trust negotiations, and federate slices. Tracking control and smooth cooperation across different planes still poses a significant challenge.

Blockchain-Enabled Architectures

The increasing needs for secure, auditable, and tamper evident orchestration have led to the incorporation of blockchain technologies into ZSM trust frameworks. Blockchain serves as an immutable and distributed ledger that captures operational activities alongside SLAs and configuration changes. This enhances accountability across both administrative and provider boundaries while facilitating clear orchestration across multiple domains. Within an orchestration domain, blockchain provides reconciled and encrypted mutable coherence [9], [14]. An accountable domain administrator can cryptographically secure, in an immutable ledger, an SLA policy, signable events, and a configuration revision, thus creating accountability in a domain of administrative overlap. Through smart contracts, SLA enforcement and monitoring on a self-governing basis can be utilized to remediate Quality of Service (QoS) violations [19], [26]. Additional measures include:

Monitoring Agents for SLA prediction assurance with Artificial Intelligence. Trust models measuring the provider's reliability through an automated reputation system [24]. Variable consensus (Proof of Stake, Byzantine fault tolerance, and Directed Acyclic Graphs) for latency reduction [9], [14].

Despite the latency, complex governance, and regulations expounded through a blockchain, Light and other off-chain layer scaling constraints are diminishing, thus it stands as a feasible trust framework for 6G zero touch system (ZSM) architecture.

Emerging 6G and Aerial Network Architectures

Aside from the secure orchestration provided through blockchain technologies, ZSM research has started to shift toward architecture innovations for 6G and Non-Terrestrial Networks (NTNs). The extreme densification of networks, AI service logic, and the introduction of aerial and satellite layers such as UAVs, HAPs, and LEO satellites create a dynamic and diverse service fabric. These ecosystems, in contrast to terrestrial deployments, have stringent latency, mobility, and reliability constraints, necessitating intent-aware, energy-efficient, and rapid reconfiguration architecture.

Core architectural innovations expected to shape 6G ZSM include:

- **Digital Twin Synchronization:** Advancements in digital twins technology enables users to create digital replicas of various terrestrial as well as non-terrestrial fabrics to prepare for abruption of service in a proactive manner by simulating failures, validating policy packs and optimizing routing. Works such as [70], [123] provides instances of digital twins for O-RAN and provide multi-domain orchestration and highlight the proactive fault management and policy validation uses of digital twins.
- **Aerial Cognitive Meshes:** Balancing the three aspects of coverage, mobility and energy efficiency as per stochastically weighted spatiotemporal metrics in the meshes is still a challenge, especially for a dynamic allocated coverage. In [32], [35], we will embark on integrating mobile UAVs with self-organization capability and base stations which change their positions dynamically to reallocate user capacity based on user activity patterns. This is in line with the coverage and mobility energy efficiency frameworks.
- **Intent-Aware Interfaces:** These frameworks focus on the problems of semantic translation and provide intent-driven solutions to the aforementioned problems [25], [92], [115]. Starting from the Asus open systems which self-optimizing module OSS, and later other modules, incorporate and demonstrate early stage functionalities using large language models, especially GPT, OSS modules are still mostly lacking semantic understanding of user commands.
- **Satellite Edge Continuity:** Dynamic edge and orbit tier seamless workload migrations using situational elements of handover, caching and layer coordination. SatCom is currently undergoing an integration within the framework of ZSM which is being researched by [83] and other surveys, and frameworks [73], [75] articulate the slice-management continuity gaps across different layers.

- **Quantum-Secure Cryptography:** With regard to the quantum environment, ensuring the confidentiality and integrity the Orchestration signal becomes paramount. This responds to [79], [109] which challenges us with preparing post-quantum systems as a priority.
- **AI-Powered Trust Fabrics:** Federated analytics that incorporate ongoing monitoring, anomaly detection, and operational resiliency across both ground and aerial domains are needed. Cyberspace federated learning [88] and lifecycle AI governance [76] suggest embedding continuous trust weaving into the orchestration of dynamic cyber-physical systems.

To conclude, 6G ZSM architectures have had to learn about emergent responsiveness, native decentralization, and enforceable auditability. The intent arbitration, cross-domain slice reconfiguration, and energy latency trade offs remain particularly complex. Still, validations in NTN settings and multi operator orchestration are relative underexplored. These are research directions we explore in RQ5.

B. AI and Automation Techniques in ZSM (RQ2)

The contributions of AI and automation have recently dominated ZSM research as detailed in the Tables I–III [3], [5], [6], [42], [47], [48]. ZSM works have primarily focused on moving from static orchestration to ML-driven closed loops, federated learning (FL), and the application of AutoML and explainable AI. The ZSM works continue to view AI as the central facilitator for achieving autonomy, optimization of decision-making, and intent satisfaction in 5G/6G systems. Learning frameworks like FL, RL, and AutoML reduce manual oversight while increasing reliability. Notable examples of this include the AutoML driven dynamic policy tuning [5], closed loop assurance [6], and the QMP [30] which integrates DevOps and MLOps for lifecycle assurance. The works provide adaptability and flexibility, but typically lack in model complexity, inter-domain latency, and reproducibility.

Distributed and Privacy-Preserving AI

FDRL [3] facilitates privacy-preserving coordinated distribution for O-RAN reconfiguration. DRL based WLAN autotuning [28], semi supervised FL for intrusion detections [29], and ensemble models for orchestrating industrial IoT [42] also promote autonomy and privacy. Nevertheless, high communication costs, training overhead, and edge resource constraints are substantial issues.

Explainability and Trustworthy AI

ZSM processes are adopting transparency in a more pronounced manner. Turbo-Explainable FL [47] improves auditability of the automation of slicing, and neuro-symbolic twins [48] facilitate IoE orchestration. Integration of XAI, albeit promising, increases latency and complexity, which hampers real-time applicability.

Lifecycle Aware Orchestration

As the SLA compliance is maintained, AI controllers monitor KPIs in real-time, enforcing policies, and recalibrating resources [6], [9]. The addition of MLOps [30] enables ZSM's reliable production AI frameworks with scalable deployment, retraining, and governance.

Intent Based Networking

Implementing AI in Intent Based Networking results in the translation of overarching objectives, such as reduced latency and enhanced reliability, into defined policies using RL and AutoML [25], [45]. Intent learning across O-RAN domains is enhanced with federated RL, providing improved scalability, although issues with semantic mismatches still exist.

Deep Learning Approaches

The backbone of the spatial temporal extraction technique is still CNNs and RNNs. CNNs and RNNs of the spatial temporal technique assists in identifying faults and anomalies, LSTMs in predicting traffic and QoS declines. RNNs and SLA predictions as well as route prediction SLA optimization have been surpassed by apparatus based Transformers. Hybrid CNN-LSTM networks augment multi modal classification, and AutoML diminish the design complexity. Federated Learning is a popular approach for privacy preserving collaborative computing at the cloud edge.

Reinforcement and Multi Agent Learning

Dynamic resource optimization and reinforcement learning for self healing with bandwidth control and scheduling. Scaling and SLA balancing is done through DQQN and policy gradient such as Actor critic and PPO. Domain extension MARL permits multi agent adaptability for cross slice MADDPG and A3C cooperative fault domain. Regulated industries benefit from adding Expose RL adding control by intent and action as XRL.

Agentic AI for Autonomous Orchestration

Agentic AI introduces goal driven reasoning agents capable of decomposing intents, planning tasks, and self-adjusting across slices [97], [100]. Frameworks such as Agent Edge [97], Agent Ran [100], and MX-AI [102] demonstrate early progress, while conceptual works envision edge general intelligence [107]. However, these remain largely simulation-bound, facing governance, safety, and reproducibility challenges.

Intent-Based ZSM

IBN enables declarative goal expression instead of device level commands [39], [41], [45].

- **Intent parsing and translation:** Transformers and AutoML interpret natural language intents into policies [10], [39], [41].

- **Intent fulfillment:** RL agents adapt bandwidth, rerouting, and scaling to maintain SLA alignment [42].
- **Fuzzy intent reasoning:** Neuro-fuzzy models manage qualitative intents acceptable quality with graded control [48].
- **Digital twin validation:** The feasibility, risks, and trade offs before deployment, deployment and after deployment as well as during the in workflow integrated phases are analyzed up by AI-augmented twins.
  item**Explainability** In scholarly works, policies are granted, and compliance is examined and subordinated as well as advance interdisciplinary supervision is integrated, advanced XAI does all this [47], [86], [89] documents.

Notable progress has been achieved in deep learning, reinforcement learning, and emerging applications of Agentic AI in Zero-Touch and Service Management, but the studied literature illustrates multiple fundamental challenges. Lightweight models such as AERO [94] prioritize simplicity and efficiency but fail to capture the broader reasoning needed for multi-domain orchestration. Agentic AI approaches [97], [100], [102] illustrate richer autonomy, but also greater unresolved governance, safety and coordination costs. Key shortcomings in both categories fell reliance on simulated environments or conceptual frameworks poorly validated in real 6G testbeds, creating a widening reproducibility gap where innovative concepts languish non empirically benchmarked. Closing this gap requires substantive algorithmic advances, as well as, standardized evaluation platforms and cross-vendor experimental validation.

C. *Security and Privacy Frameworks (RQ3)*

The academic literature concerning and focusing specifically on security and privacy in the context of the Zero Touch Service Management (ZSM) and 6G ecosystem domains is systematically consolidated across multiple thematic domains, each examining interrelated matters of smart automation and intelligent orchestration of security.

Table I incorporates such components as Zero-Trust Architecture, the robustness of Federated Learning, and the orchestration of security domains, elucidating the association of ZSM mechanisms with self-defensive, adaptive, policy based shields [2], [8], [12], [19]. Further Review focus into the industrial sphere namely, zero-trust for the IIoT [42], slice optimization and security embedded intent-based networking [39], [45], and explainable AI or trustworthy 6G operations with interpretable large language models [34]. This also covers satellite ZSM constraints [35] and the security sustainability trade off [46].

In Table IV, privacy preserving orchestration arises from secure credential [62], [64], multi tenant RAN sharing [63], and the 6G roadmap [65], [66]. Table VI integrates O-RAN security [86]–[88], the function of Digital Twins in riskless O-RAN testing [70], [71], and energy angles [72], [74]. Table VII focus on governance, trust, and LLM governance cross-cutting [89], [90], [92], [109], the collection on 6G security, differential privacy FL [121], and DT based assurance frameworks [123].

Zero-touch security in slicing and UAV networks:

Isolation and mobility management are crucial, and strong boundaries are needed because slicing and edge networks using UAVs are emerging as zones of high risk. Fore described mobility control and scale aware orchestration [31] improves reliability, however, energy and interoperability constraints still exist. Neutral host designs [63] add openness, however, the risk of tenant policy conflicts still exist.

AI-driven adaptive defenses and explainability:

Automational security integrated and characterized with Artificial Intelligence as an anomaly detection service and XAI/LLM used for trust and attribution, are deployed across multiple levels of an architecture as AI-as-a-Service [33]. Their shortcomings primarily related to computational costs and excessive synthesis are outweighed by their advantages of scalability and understandability. The O-RAN research [118], [119] lay open practical weaknesses; the Digital Twin validation [70], [123] assists to alleviate the risk of phased deployment.

Cross-domain privacy, trust, and governance:

Privacy by design is enabled through IIoT zero-trust ensembles [42], privacy preserving credentials [62], [64], and DP-FL [121] as noted in the preceding paragraph. However, the persistent problem of training overheads and uneven compliance within the domains fail to disappear [120].

Observed Limitations (RQ3):

- Cross-slice isolation and scalability remain undertested.
- IoT/UAV domains face feasibility and energy bottlenecks.
- XAI/LLM pipelines introduce latency and safety overheads.
- Fragmented implementations across physical and service layers hinder integration.

1) ZSM Security Considerations and Their Privacy Concerns

Security and privacy are foundational to Zero-Touch Network and Service Management, particularly due to the inherent automation, cross-domain orchestration, and decentralized decision making it entails. As networks transition into highly dynamic, AI-driven architectures under 5G/6G, traditional perimeter defenses are insufficient. This section reviews four pillars that recur across our evidence tables:

- AI-powered intrusion detection,
- privacy-preserving learning,
- explainable AI (XAI), and
- trust/governance mechanisms (for example, ZTA, credentials, privacy by design orchestration).

*2) **AI-Powered Intrusion Detection and Threat Response***

Artificial Intelligence and Machine Learning increasingly underpin next generation intrusion detection systems for ZSM. Unlike static, rule based IDS, AI-enabled models adapt to non stationary traffic and service dynamics, which is essential for automated orchestration. As reflected in Tables, leading directions include: AutoML-driven security analytics [5], federated learning for IDS [29], and explainability infused models for operator accountability [34], [36], [47], [57], [86], [88].

Deep learning backbones such as CNNs, autoencoders, and LSTMs support traffic anomaly detection and fault localization with minimal operator input, while ensemble methods strengthen resilience against high-dimensional IIoT attack patterns [42]. Recent systems incorporate transformer-style encoders and attention to capture long-range temporal dependencies in telemetry streams see [42] for adaptive ensembles, and the XAI over viewed pipelines in [36], [86].

Practical constraints and remedies.

- Limited labeled data: Real 5G/6G traces with ground-truth attacks are scarce. FL-based and semi supervised approaches [29], [88] mitigate label scarcity and data-sharing restrictions by learning collaboratively without centralizing raw data.
- Edge resource budgets: Heavy DL models strain MEC/edge nodes. FL architectures [60] and lightweight inference (pruning/quantization) reduce on-device cost while maintaining utility; DP-FL adds privacy but may slow convergence [121].
- Operator trust: Black box alarms hinder human oversight. XAI (for example, attribution or heatmaps) improves traceability in IDS and slicing control loops [34], [36], [47], [86], with TEFL [47] illustrating explainability directly integrated into FL pipelines.

Integration into ZSM closed loops. AI-powered IDS is increasingly embedded into ZSM orchestration:

- Federated/Split IDS: collaborative anomaly detection across domains without sharing raw data [29], [60], [88], [121].
- Zero-Trust enforcement: least privilege, continuous verification across multi-tenant slices and edge domains [2], [11], [77].
- Identity and privacy controls: attribute-based credentials (ABC) and privacy-by-design orchestration limit metadata exposure during cross-domain actions [62], [64].

*3) **Blockchain for Trust, Transparency, and Governance***

Increasingly, Blockchain technology is seen as an important component of ZSM regarding trust and transparency. By maintaining a ledger that cannot be altered or destroyed, and that is supported by verifiable orchestration logs and policy compliance across multiple administrative domains, blockchain technology complements orchestration logs [56]. This decentralized system of trust models ZSM enables auditing on: SLAs, configuration changes, and operational activities. Table XV summarizes the benefits and drawbacks of blockchain technology on cross domain accountability, trust, and zsm performance.

The primary benefit is the use of smart contracts that automate SLA configuration and enforcement by changing the system state upon the satisfaction of triggers [56]. This type of automation creates blame-free environments, where stakeholders can be assured that their defense and dissenting positions on the system state evolution, triggered by the set of conditions, will not be altered.

Integrating ZSM with Blockchain is a complex undertaking with a number of unresolved issues. This is indeed a paradox as a number of practical issues still exist Table XV.

The need for speed in real-time orchestration versus blockchain networks. Studies [63], [64] confirm that ultra-reliable low-latency communication can be significantly impeded by confirmation delays. Protocols at Layer 2 like sidechains and rollups are beginning to be used to boost transaction throughput without sacrificing integrity. In these environments, consensus mechanisms like Proof-of-Work are both remote and impractical due to their immense resource and energy demands optimally processing these algorithms. Proof-of-Authority (PoA) and Delegated Proof-of-Stake (DPoS) are mechanisms, to name a few, that have been put forth to alleviate some consensus resource expenditure without compromising security and integrity [65]. Integration of blockchain technology within existing systems is often made intricate by the presence of older interoperable systems which were not designed with blockchain technology in mind. These older systems coupled with other systems result in what is termed the hybrid on-chain or off-chain models, which lately seem to be gaining traction. Such models are ideal in cases where only crucial events (such as SLA violations) need to be anchored on chain, while all other routine tasks may be orchestrated off-chain to streamline the entire process and decrease the system's latency.

Blockchain in ZSM is promising for accountability, trust, decentralized governance, and transparency. However, as indicated in Table XV, these advantages come with serious sacrifices in scalability, latency, and integration complexity. Future works needs to address the binding of blockchain with the trust properties to the performance needs of 6G orchestration.

*4) **Privacy-Preserving AI via Federated Learning and Differential Privacy***

Within ZSM, protecting privacy and confidentiality is imperative due to the sensitive nature of information that is exchanged among operators, edge devices, and service domains. This is more pronounced within regulated domains, including, but not limited to, the politic military domains, healthcare, and industrial automation, as well as smart infrastructure [66]. Federated Learning is touted in several studies as a privacy preserving model as described in Table XV, where models are trained locally and only model parameters

TABLE XIV List of Acronyms

Acronym	Definition
SDN	Software-Defined Networking
NFV	Network Function Virtualization
VNF	Virtualized Network Function
SD-WAN	Software-Defined Wide Area Network
SBI	Service-Based Interface
API	Application Programming Interface
TOSCA	Topology and Orchestration Specification for Cloud Applications
YANG	Yet Another Next Generation (data modeling language)
MEC	Multi-access Edge Computing
RAN	Radio Access Network
O-RAN	Open Radio Access Network
UAV	Unmanned Aerial Vehicle
HAP	High-Altitude Platform
NTN	Non-Terrestrial Networks
LEO	Low Earth Orbit
QoE	Quality of Experience
QoS	Quality of Service
SLA	Service-Level Agreement
KPI	Key Performance Indicator
CDR	Call Detail Record
ZT	Zero Trust
ZTA	Zero-Trust Architecture
IDS	Intrusion Detection System
ABC	Attribute-Based Credentials
GDPR	General Data Protection Regulation
EU AI Act	European Union Artificial Intelligence Act
SHAP	SHapley Additive exPlanations
AIaaS	AI as a Service
IoT	Internet of Things
IIoT	Industrial Internet of Things
URLLC	Ultra-Reliable Low-Latency Communications

Acronym	Definition
5G	Fifth-Generation Mobile Network
6G	Sixth-Generation Mobile Network
B5G	Beyond 5G
eMBB	Enhanced Mobile Broadband
mMTC	Massive Machine-Type Communications
ZSM	Zero-touch Network and Service Management
IBN	Intent-Based Networking
E2E	End-to-End
IoE	Internet of Everything
M&O	Management and Orchestration
AI	Artificial Intelligence
ML	Machine Learning
RL	Reinforcement Learning
DRL	Deep Reinforcement Learning
FL	Federated Learning
MARL	Multi-Agent Reinforcement Learning
MLOps	Machine Learning Operations
XAI	Explainable Artificial Intelligence
LLM	Large Language Model
CNN	Convolutional Neural Network
RNN	Recurrent Neural Network
LSTM	Long Short-Term Memory
DT	Digital Twin
DQN	Deep Q-Network
PPO	Proximal Policy Optimization
A3C	Asynchronous Advantage Actor-Critic
MADDPG	Multi-Agent Deep Deterministic Policy Gradient
ERP	Enterprise Resource Planning
XR	Extended Reality
CI/CD	Continuous Integration / Continuous Delivery
ETSI	European Telecommunications Standards Institute

are sent to the central server for aggregation [71]. This approach guarantees that the sensitive information will not leave its geographical location, thus satisfying the criteria of GDPR and other privacy legislation in force across the world.

As promising as it is, FL is subject to many risks. Attacks such as gradient inversion, membership inference, and poisoning attempts can unmask sensitive data. In order to constrain these risks, Differential Privacy has been applied to the FL pipelines. With the addition of noise that is mathematically bounded, DP prevents the identification of clients and data contributors during aggregation [62], [74]. These methods, as seen in Table XV, are classified as strong privacy protections.

Beyond FL and DP, research identifies several practical solutions to address persistent challenges:

- Model inversion and gradient leakage: exposure is limited by secure aggregation protocols which prevent the central server from accessing updates from individual clients.
- Federated settings row clients: the Byzantine-resilient aggregation and anomaly detection techniques assist in the identification of poisoned and malicious updates.
- Efficiency in training: advanced techniques in model compression (quantization, pruning, and sparsity) alongside strategic client selection which suppresses the communication overhead. This is achieved in distributed deployments [60], [88].

5) Explainable AI for Regulatory and Operator Trust

AI automations are core to the essence of Zero-Touch Network and Service Management, and the need to provide explainability is essential to operational transparency and compliance with regulation, and human oversight [73], [76]. Most orchestration frameworks are built using deep learning or black box ensembles, which yield impressive predictive accuracy, but little to no explainability. Lack of transparency

TABLE XV Comparison of security and privacy mechanisms in Zero-Touch Network & Service Management.

References	Security / Privacy Technique	Targeted Threats	Privacy Protection	Underlying Technology	Key Advantages / Notes
[2]	Zero-Trust architecture (5G+)	Impersonation, lateral movement, unauthorized access	**Yes** (least-privilege, continuous verify)	PDP/PEP, continuous auth/attestation, policy enforcement	End-to-end ZT posture across lifecycle
[5]	AutoML for security analytics	Model drift, evolving threats	Partial	AutoML pipelines for security tasks	Faster iteration; improved accuracy/latency
[11]	ZT at IoT edge (SDN-assisted CPS)	Compromised nodes; control-plane abuse	Yes	ZT controls on edge; SDN integration	Fine-grained, context-aware access
[20]	Telemetry-driven assurance	SLA violations; faults	Partial	Closed-loop with SDN/NFV/MEC analytics	Assurance-ready architecture
[24]	ZT/AI/ML for IoT security	IoT attack surface; data exposure	Strong	ZT frameworks; optional blockchain	End-to-end IoT posture
[29]	FL-empowered IDS	Intrusions with scarce labels	Strong	FL + semi/active learning	High detection; robust aggregation needed
[34]	XAI+LLMs for trustworthy ZSM	Opaque automation	Partial	XAI + LLM pipelines	Operator transparency
[36]	XAI for 6G (survey)	Lack of explainability	Indirect	SHAP/LIME/IG	Method guidance
[37]	Open RAN security	Supply-chain/config risks	Indirect	O-RAN threat model	Hardening guidance
[42]	Ensembles + ZT provisioning (IIoT)	IIoT cyberattacks; QoS contention	Partial	Adaptive ensembles	Better resilience
[47]	TEFL for slicing	Opaque/poisoned FL	Strong + XAI	FL with explanation-aware constraints	Trustworthy slice decisions
[60]	Split/federated learning	Data leakage; device limits	Strong	Split FL; secure aggregation	Privacy by design
[62]	Attribute-based credentials	Linkability; over-disclosure	Strong	Verifiable/ABC credentials	Fine-grained access
[64]	Privacy-aware orchestrators	Cross-domain metadata leaks	Strong	Privacy policy extensions	Interop privacy in flows
[65]	Secure 6G roadmap	Evolving threats; governance	Yes	Identity/micro-segmentation	Strategic alignment
[70]	Digital twins for O-RAN	Unsafe rollout/config errors	Indirect	Twin-based "what-if"	Safer changes
[77]	Zero Trust for 6G	Insider/cross-layer gaps	Yes	ZT patterns mapped to 6G	Architectural guidance
[79]	Cross-layer automated security	Misconfigurations; multi-layer attacks	Partial	Intent-linked security	Security–automation bridge
[85]	Secure low-latency IoT	Latency/privacy tensions	Partial→Strong	Edge analytics; DP options	IIoT-friendly privacy
[86]	XAI in O-RAN	Opaque RAN control loops	Indirect	XAI for RAN/slicing	Auditability/trust
[87]	LLMs in 6G security	Misconfig/data leakage	Partial	LLM-assisted SecOps	Faster triage; risk taxonomy
[88]	FL for cybersecurity	Poisoning/backdoors	Strong	Robust aggregation defenses	Best practices for secure FL
[89]	LLMs for comms mgmt	Intent/policy ambiguity	Partial	LLMs across OSS/BSS	Natural-language ops; guardrails

to the system's logic is a risk in heavily regulated or mission critical conditions, especially where understanding decision rationales is needed, and the decision is automated.

Though lacking comprehensibility, Explainable AI frameworks focus on providing some form of insights into how the models work. The more popular ones, SHAP and LIME, focus on decomposing outputs and attributing individual features. This allows operators to make sense of the decision paths and audit orchestration pipelines. Works summarized in Table XV rows [34], [36], [86] address the importance of XAI in ZSM from surveys and methodology to LLM-augmented orchestration pipelines for improved transparency.

Key applications of XAI in ZSM include:

- Functional justification: detailing the reasons a slice was modified from its original path or terminated to help operators confirm the alignment to the SLA.
- Root cause analysis: identifying the causes of orchestration deficiencies from logs which can be understood without specialized knowledge.
- Regulatory compliance: ensuring the documented rationale captures compliance to the GDPR, ISO/IEC 27001, and the EU AI Act.

Figure 8 Analyses security techniques on various ZSM dimensions and concludes that while XAI augments transparency and trust, it is still less effective than techniques, such as federated learning, regarding privacy guarantees. Survey results indicate that upcoming ZSM platforms will need to integrate Domain specificXAI within the orchestration engines constructed for ZSM. Also, they will need to reconcile interpretability and latency, and align automation with regulatory and ethical paradoxes.

6) Ethical AI Governance in ZSM

As Artificial Intelligence is increasingly deployed in orchestration along with Federated Learning on Zero-Touch Network and Service Management Systems, increased autonomy on network and service them poses a challenge on how ethical governance is framed regarding the use and application of the Technology. Within the governance architecture, the ZSM must be beyond effective and also ensure that fairness, transparency, privacy and other standards on ZSM are adhered to [8], [18]. Ethical AI now appears to be a governance architecture for the cross domain structural pillars which includes Technology of Automation, Security, and Intent Based Management.

Bias Mitigation

The presence of bias in training data and inferences from the model can compromise equity in ZSM decision automation. To mitigate the issue, explainability and fairness metrics are being incorporated within orchestration pipelines. For example, SHAP aided explainable orchestration for network slice admission control provides clarity and justification for policy making decisions [18]. Differential privacy can reduce demographic or geographic discrimination bias in FL training [24]. These methods maintain attribute level privacy at the network edge, safeguarded, thus reinforcing equity and data usability.

Regulatory Compliance

Adhering to data protection and AI guidelines is one of the most important aspects of ethical ZSM. Federated learning platforms practice data decentralization and comply with the data protection by design principles [8]. Policy engines with explainable AI can fulfill decision traceability and service chaining orchestration as automation objectives outlined in the ETSI ZSM workstreams note [12], [30]. Federated and explainable AI, in Table XV, becoming more integrated with modular frameworks and architectures, intent-based networking, and blockchain emphasizes their importance in the governance.

Implementation Challenges

The introduction of real time fairness aware orchestration increases latency. Cross jurisdictional compliance adds complexity, as deployments must balance GDPR. The lack of aligned policies increases the risk of fragmentation in the federated governance layers. Table XV illustrates this tension: while numerous ZSM studies focus on lifecycle automation and fault management, less attention is paid to privacy and ethical governance in an integrated manner.

The incorporation of fairness metrics, explainable AI, and federated governance is starting to become essential for scalable ZSM. However, as noted in Table XV, much research is still overly focused on the automation and performance of ZSM systems. The next generation of ZSM systems is expected to incorporate governance as a primary design factor, aligned with trust and legitimacy in AI-driven networks: cross-border bias remediation, regulatory compliance, and inter jurisdictional governance.

D. Service Lifecycle and Cross-Domain Management (RQ4)

Lifecycle automation contributions are captured in II [31], [35]–[37] extended in III [38], [39], [41], [43], [51] and further in V [73], [75], [76]. These collectively show how onboarding, assurance, scaling, healing, and decommissioning are being redefined under AI driven, intent-based, and cross-domain orchestration. More recent contributions [114], [120] emphasize privacy preserving FL for lifecycle assurance and adaptive governance in vehicular and industrial testbeds.

AI based lifecycle automation

[35] demonstrates AI based zero-touch management for satellite networks, introducing intent translation and closed-loop provisioning across non-terrestrial and terrestrial domains. In Table II, this is flagged as supporting space infrastructure but limited by latency and intermittent connectivity. Similarly, [9] emphasizes lifecycle AI covering service design to assurance; its strength is holistic lifecycle coverage, while its limitation is high operational overhead. Complementary surveys [111] confirm that satellite lifecycle automation still lacks cross operator validation at scale.

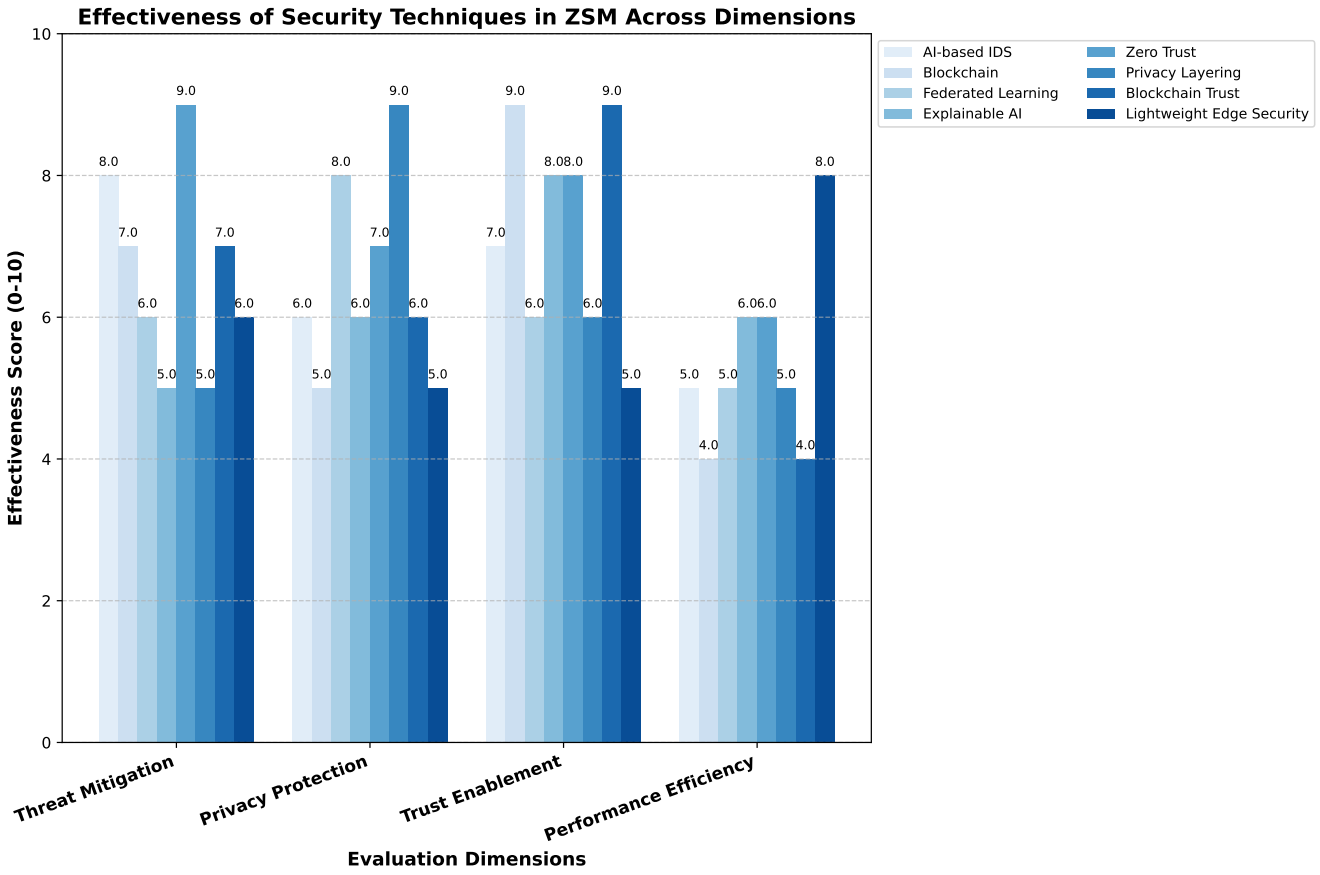

Fig. 8: Comparison of security techniques across ZSM dimensions. Techniques such as FL provide strong privacy, while XAI emphasizes interpretability and operator trust.

Transparency and compliance

Lifecycle pipelines increasingly embed Explainable AI. [36] integrates XAI to enhance interpretability in orchestration, crucial for compliance heavy verticals (healthcare, vehicular, energy). This is identified as improving decision trust but still conceptual and early-phase. Broader surveys [120] reinforce that accountability and compliance remain under standardized in lifecycle management.

O-RAN and lifecycle governance

Lifecycle automation in O-RAN introduces governance and interoperability risks. [37] categorizes security threats in open RAN architectures, offering a clear taxonomy of vulnerabilities. As per Table I, this provides threat awareness but few validated countermeasures. Later, [118] empirically validated lifecycle vulnerabilities via stress testing of ONOS and OSC RICs, while [119] advanced layered defense models. Together, these works move from taxonomy $\rightarrow$ empirical testing $\rightarrow$ structured defense proposals, but lifecycle enforcement in O-RAN remains incomplete.

Industrial and cross domain use cases

Beyond telecom, lifecycle automation extends into Industry 5.0 and smart factories. [38] proposes XAI-based orchestration to align with human centric Industry 5.0 principles. Likewise, [73] introduces scalable AI driven slice management, and [76] emphasizes lifecycle AI governance (REASON approach). Recent surveys [114] confirm that most industrial lifecycle models remain proof-of-concept.

Slice optimization as enabler

Slicing is central to lifecycle orchestration. [39] introduces ML-driven dynamic slice optimization for SLA compliance, as practical and effective, though tested in limited environments.

Observed limitations (RQ4)

Across Tables I–VIII, four consistent gaps emerge as high operational overhead in lifecycle AI orchestration [9], limited validation for satellite and Industry 5.0 lifecycles [35], [38], interoperability and scalability gaps in O-RAN lifecycle governance [37], [118], [119], and insufficient integration of FL/privacy and compliance frameworks into production-ready lifecycle systems [76], [120].

Collectively, lifecycle automation in ZSM is progressing from conceptual AI-based orchestration [9], [35], [36], toward governance and O-RAN-specific risks [37], [118],

[119], and industrial cross-domain contexts [38], [73], [76]. To achieve trustworthy lifecycle automation in 6G, future work must reduce operational overhead, validate in multi-domain testbeds, and standardize privacy/compliance mechanisms.

*1) **Cross-Domain Service Lifecycle Management***

Cross Domain Service Lifecycle Management supports ZSM by automating service onboarding, activation, assurance, optimization, and decommissioning over diverse infrastructures. It needs cross domain collaboration dealing with different orchestration logics, security postures, and SLA boundaries: fragmentation and SLA breaches surface when harmonization does not occur.

Works like [1], [75] achieve end-to-end orchestration with SDN and NFV and MEC and AI analytics, and intent driven frameworks [13], [45] foster high altitude goal decomposition into workflows and retain a high degree of manual conflict resolution. Federated and privacy preserving frameworks [8], [29] apply Zero-Trust security, while cloud native approaches [30], [41] promote microservices and self-governing loops for generous scalability. The Outstanding problems of [31], [75] orchestration fragmentation, intent translation bottlenecks [13], [25], and distrust across domain boundaries [2], [62] remain across these works. Standardized intent semantics with Zero-Trust woven throughout and federated assurance fabrics recapturing state across providers begin to emerge.

Current methodologies optimize separate lifecycle portions, for example, orchestration. Future ZSM systems should distribute lifecycle management across all phases, ensuring privacy, explainable governance, and seamless, reliable service across 6G environments.

*2) **Service Onboarding and Activation***

Service onboarding starts with registration, validation, and configuration which is required before set up can begin. In multi domain scenarios, onboarding needs to tackle descriptor heterogeneity (TOSCA, YANG, NSD), protocol diversity (REST, gRPC, NETCONF), and conflicting intents. Still, the portability of intent is quite limited; vendor-specific models lack interoperability and cause issues with conflict resolution. Semantics aligned with ETSI/TM Forum, augmented by AI-driven translation and conflict reconciliation, are critical for automated scale. Service onboarding processes are improving from descriptor centric, static deployments to intent-driven, orchestrated APIs. However, models still lack structure and fragmentation is rampant. Future studies should focus on conflict aware intent translation, descriptor standardization, and alignment with cross reach onboarding governance for true multi-domain integration.

*3) **Service Assurance and Fault Management***

Continuity in performance, and reliability across distributed domains [4], [6], [12] for service assurance allocates resources for different domains. Monitoring, SLA enforcement, anomaly detection, and automated remediation are functionalities achieved in real-time. Reconciling differing assurance policies and asynchronous telemetry across domains is the tough part. AI/ML techniques take center stage across all domains. Predictive fault detection for maintenance [12], [49] using LSTMs, autoencoders, and graph neural networks, and complex closed-loop self-healing [6], [51] systems take care of automated recovery. RCA is augmented with interpretable justifications by XAI [57], [66].

Core Components:

- **Telemetry Aggregators:** Collect multi-source metrics (jitter, latency, throughput) for SLA compliance.
- **Policy Enforcement Engines:** Apply automated or human-approved mitigation when thresholds are breached [20].
- **Federated Monitoring:** Enable local governance while maintaining global SLA assurance [60].

As indicated by [63], time aligned notifications are ensured by the use of standardized event schemas (ETSI SOL005) and streaming buses (Kafka). Digital twins simulate the service behavior with faults to validate the resilience of the service before deploying.

Service assurance still stands to be one of the most fragmented stages of the lifecycle [9], [29]. AI driven anomaly detection [9] and monitoring based on federated learning [29] are highly promising tools on their um, but lack integration with policy enforcements of intent-driven orchestration and Zero-Trust for scaleable and reliable explainable I guess performance.

*4) **Service Decommissioning and Optimization***

According to the external source [4], [20], the last step in the lifecycle which is the 'decommissioning' phase involves the dismantling of instances, removal of policies, and the reclamation of computing, memory, and network resources. There is also the need to address the synchronized state confirmation, rollback of configurations, and termination compliance in the domains of cross-domain environments [20]. Starting from cloud-native decommissioning and orchestrations engines [9], [10], [30], [41], the table captures and details workflows automating decommissioning through SLAs, intent withdrawal, and resource expiry. These workflows assist in the unbinding of resources, deletion of containers in Kubernetes-based configurations, and IP/volume/metadata reclamation, to cite a few. Policy-based clean-up rules enforcement of retentions, separation migrations, and deletion suppression windows during service transition helps enhance flow [59]. In contexts whereby latency is deemed the most important, frameworks incorporating reinforcement learning like DDPG based orchestration [54] have aimed to optimize reclamation of resources in order to alleviate starvation scenarios while increasing overall system efficiency.

In the table the gaps in lifecycles shows the continuing issues in legacy integration cross border synchronizations [1], [55]. Automating reclaiming of resources is the focus of most available approaches but governance and compliance testing, trust validation, and proof decommissioning reclamation flow significantly lags behind. Audit transparency and decommissioning workflows are crucial for the ac-

TABLE XVI Service Lifecycle Gaps and Strategic Solutions in ZSM

References	Gap Category	Challenges	Strategic Solutions
[31], [75]	Service Orchestration Fragmentation	Fragmented orchestration across vendors/domains; limited end-to-end service state visibility leading to SLA breaches.	• Cross-domain orchestration and slice federation via open interfaces/domain managers. • Distributed service fabrics and state reconciliation across domains (event-driven coordination).
[13], [25]	Intent-Based Provisioning Limitations	Vendor-specific intent models, lack of shared semantics, and poor portability across orchestrators.	• Standardized/semantic intent models (ETSI/TM Forum alignment). • IBN pipelines to translate goals into executable policies with conflict handling.
[1], [55]	Legacy System Integration	Proprietary OSS/BSS interfaces; limited inter-operation with NFV/SDN and cloud-native orchestrators; heterogeneous service/element descriptors.	• Standards-based north/southbound interfaces (e.g., ETSI MANO descriptors, YANG models) plus adapter/gateway patterns for legacy OSS/BSS. • NFV/SDN-aligned element management to bridge legacy NMS/EMS with modern orchestration.
[9], [29]	Lifecycle Assurance and Monitoring	Limited automation in cross-domain assurance; hard KPI correlation across heterogeneous domains.	• [9] AI/ML anomaly detection and predictive assurance. • [29] Federated learning for privacy-preserving KPI/model sharing across domains.
[2], [62]	Security and Trust in Lifecycle Operations	Inter domain handovers and control plane exchanges expose trust gaps; risk of unauthorized/malicious updates and false state propagation.	• Zero-Trust architecture with continuous verification (identity, device posture, least-privilege) across lifecycle steps. • Privacy-preserving attribute-based credentials for selective disclosure and verifiable, revocable access in orchestration.

countability that ZSM in 6G context requires, while privacy preserving orchestration are needed.

*5) **Dynamic Optimization and Cost Efficiency***

ZSM systems must not only perform resource cleanup, but also continuously optimize services to achieve an optimal balance among performance, latency, and operational cost. As discussed above dynamic optimization frameworks use analytics and artificial intelligence-enabled heuristics to:

- Monitor underutilized instances and recommend consolidation to minimize orphaned capacity.
- Anticipate maximum loads and perform VNFs or CNFs provisioning elastically.
- Optimally redirect traffic to facilitate economical routing for regional inter-domain traffic optimization and to minimize outbound inter-domain link traffic.

Observation frameworks that incorporate KPIs metric to closed-loop orchestration rely on Reinforcement learning (RL) agents that optimize policies to minimize total cost of ownership (TCO) while satisfying SLA obligations. This motivation is vital in edge and tactile-internet cases where service SLA is bounded by strict latencies and service level energy constraints [49], [51], [52]. In 6G ready context where computation is limited and needs to be shared, ZSM platforms utilize:

- Elasticity policies that favor latency-sensitive services while deprioritizing latency-insensitive services.
- Adaptive timeouts and on-demand instantiation that shorten inactivity to minimize waste and optimize economic efficiency.
- Slice-aware deactivation rules that in multi-slice 6G contexts selectively switch off dormant resources [58], [63].

RL and AI augmented frameworks show impressive siloed cost attributes, still need to improve in cross domain comprehensiveness and transparency. Current systems still granularly assign cost optimization to users and verticals while fundamentally multi-domain economics remain completely underutilized. Explainable cost-latency optimization models, and federated cost optimization across the tiers are poorly understood and attributed to system ZSM lacking sustainability.

*6) **Unified Lifecycle Governance***

The ZSM evolution anticipates unified lifecycle governance, involving onboarding, assurance, scaling, optimization, and decommissioning within a managed control plane. studies highlight that future-proof architectures consolidate:

- **Intent-to-Policy Engines:** Converting business objectives to executed orchestration logic [13], [25].
- **Domain Agnostic Lifecycle Managers:** Facilitating cross-vendor orchestration via standard, open interface descriptors [1], [55].
- **AI Enabled Adaptive Loops:** Modifying services based on predicted or observed conditions within and across networks [30], [41]

.

Such unified frameworks are essential to ensure SLA compliance, sustain resilience, and facilitate auditability of compliance in regulated contexts. These frameworks are also becoming more aligned with parallel initiatives in O-RAN, privacy-preserving orchestration, and secured multi-domain governance [62], [64], [65], [67].

Although there has been progress, current governance models are still fragmented, with intent resolution, explainability, and cross jurisdictional compliance bottlenecks burning as most severe. Sustainably keeping ZSM at scale without intent ambiguity and auto-orchestration with divisible semantics are exemplified by the practical problem highlighted in lifecycle automation. These are sophisticated challenges befitting the seamless integration of domain specific explainable AI, federated compliance frameworks, and trust empowered orchestration, marking the attainment of ZSM for 6G.

E. Emerging Technologies and Future Research (RQ5)

The future oriented ZSM contributions can be found in Table I rows [15], [17] and extended in Table III rows [45], [48] and Table V rows [70], [73], [75], [76], [80]. These works envision ZSM evolution through intelligent assurance and digital twins, intent-driven orchestration, and through quantum or LLM powered frameworks. More recent perspectives that [118]–[120] have published reinforces these directions by validating O-RAN security testbeds, proposing layered governance for quantum orchestration, and framing accountability in the governance of standardization pathways. Emerging paradigms such as Edge-native Intelligence, Semantics-driven Orchestration, and Quantum-resilient AI models are aimed at resolving the scalability, transparency, and adaptability gaps in the current architecture. Use-centric intelligent service assurance, as exemplified in multimedia-focused models [15], enhances automated QoE monitoring, while smart-highway testbeds enable real-time vehicular orchestration [17]. These are under QoE ML and Smart City ZSM, with stressing real-time adaptability and targeting contextmspecific tuning and generalizability. In broader standardization pathways that [120] discusses, such enablers are framed, but the noted regulatory clarity is behind the technical progress.

Digital Twins Alongside Holographic Services:

Use cases like holographic telepresence and digital twins [22] on the other hand, require constant modification devoid of human intervention. Digital twin frameworks as shown in [69] are aligned with 6G visions, but digital twin frameworks are associated with some form of conceptual and unresolved implementation complexity issues. Similarly, anticipatory designs are emphasized in AI privacy and quantum resilient models [26], but as affirmed in II, they are still pending. Quantum masters orchestration concepts [119] suggest layer threat models, but remain speculative as there is little evidence of pragmatic hardware backed attempts.

Cross Domain Orchestration and Knowledge Sharing:

Multi domain AI orchestration as proposed by [27] facilitates domain spanning knowledge and agent collaboration. In Table I as Cross Domain AI, the orchestration gaps are attributed to architecture design deficiency. Intent-based frameworks [45] in Table III, IBN includes AI and goes further to defend space terrestrial convergence, albeit with integration complexity hurdles. Recent experimental insights [118] from near real time RIC security tests confirms the complexity of integration is not merely conceptual, but a reality to be grappled with to create interoperable systems.

Intent semantics and ontologies:

And still, intent translation into policies, as exhibited in works by [25], [45] create even more allure for intent-based networking automation, as it remains fundamental. The ambiguity in intent semantics and a lack of standardized ontologies remain obstacles to a wider adoption of this intent concerning the early intent detection of LLMs, as illustrated in Table VI row [92]. The anticipation around this innovation still remains speculative, and is surrounded by a fog of uncertainty.

Observed limitations (RQ5):

Despite the optimism and forward-looking contributions, the observed limitations consist of holographic use cases in the digital twin, scalability limitations, quantum or LLM-based orchestration knowledge gaps, cross-domain or IBN systems integration complexity (validated in the RIC testbeds), and the absence of standardized ontologies for translating semantic intents.

*1) **Emerging Research Trends and Future Directions in ZSM***

With the development of the next generation of mobile technologies (6G) over the current generation (5G), the demands placed on Zero-Touch Network and Service Management for flexibility and automation have shifted. Increased edge network processing capabilities along with the deployment of hybrid AI systems, terrestrial aerial network integration, and other standardization activities drive this change. This passage describes and synthesizes the implications of these technological advancements for the evolution of ZSM.

*2) **6G Network Management Challenges***

6G networks will change the paradigms set by 5G networks. Since 6G will come with non-terrestrial networks, ultra-dense hyper-connected environments, and new use cases like autonomous systems, the tactile internet, and holographic communications [22], [70], [78], [83]. Such environments will need zero-touch orchestration systems designed to self-manage intricate, fluid, and sometimes intermittently connected systems. They challenges for these networks are categorized under 6G Use Case Readiness, Agentic AI & LLM-Orchestration, and Security and Privacy.

Specifically, 6G will demand ZSM systems that handle:

- **Layered Mobility:** Real-time orchestration across heterogeneous nodes including satellites, UAVs, aerial edge meshes, and LEO segments, ensuring seamless mobility and service continuity [83], [97].
- **Intermittent Connectivity:** Robust failover, opportunistic routing, and store-and-forward mechanisms for disconnected or delay-prone NTN or vehicular scenarios [52], [83].
- **Hierarchical Resource Management:** Coordinated orchestration spanning satellite beamforming, UAV relays, terrestrial backhaul, and multi-domain edge tiers. Agentic and XAI frameworks provide interpretable, adaptive resource control [99], [100].
- **Semantic Intent Translation:** Goal-driven orchestration must resolve ambiguities in translating service intents into executable policies. LLM-based orchestrators (e.g., OSS-GPT, LLM agents) enable cross-layer task automation but raise governance and efficiency concerns [89], [113], [115].
- **Resilience and Trust:** As orchestration grows autonomous, zero-trust architectures (ZTA) and privacy-preserving federated learning need to be natively integrated to secure multi-domain slices [2], [8], [121].

Traditional static or rule-based paradigms are insufficient for these dynamic environments. ZSM in 6G must be inherently cognitive, self-adaptive, and resilient. AI-driven traffic steering can dynamically shift flows between orbital and terrestrial paths based on SLA priorities and latency budgets [35], [83], while agentic controllers [97], [101], [102] and LLM-based orchestrators [113], [115] illustrate real-time, explainable decision-making.

*3) **Solutions and Research Directions***

Recent research explores the following solution paths and open research directions:

- **Digital Twin Enabled Network Planning:** Predictive evaluation in simulation-driven testing of orchestration strategies helps in the use of digital twins of 6G infrastructure (O-RAN, edge, satellite) for analysis under diverse dynamic loads and topologies [69], [70]. These models, as noted in the table under 6G Use Case Readiness, enhance adaptability but remain contour heavy and are in need of large-scale validation.
- **Cognitive Multi Agent Orchestration:** Multi agent and reinforcement learning models deployed across hierarchical layers (ground, edge, aerial) facilitate the support of decentralized decision-making along with synchronized state maintenance.
- **Energy-Aware Automation:** Energy optimized orchestration [72] drives the adaptive resource allocation for aerial and satellite nodes while still meeting the defined QoE/SLA targets. As noted under Scalability and AI Efficiency, such strategies enhance sustainability, however, they cause an increase in latency and reduction in resource elasticity.
- **Zero-Touch Service Federation:** Facilitates cross-domain federation for seamless handoff, service migration, and the trust negotiation process across 6G segments that are independently managed [73], [75]. Cross-Domain Orchestration is marked as a scalability cornerstone, but is hampered by the lack of regulatory cohesion between disparate operators.
- **Quantum-Secure ZSM Models:** Integrating post-quantum cryptography with zero-trust controls, such as privacy-preserving credentials and federated learning, enhances the ZSM control planes' resilience [65], [77]. Trust anchors are definitely ensured as mapped under Security and Privacy, yet integration complexity coupled with computational overhead remains a concern.

*4) **Real Time Data Processing and Edge Analytics***

Instantaneous real time data processing at the edge is critical for super responsive ZSM, particularly for the autonomous transport, industrial IoT, tactile or holographic, safety and emergency communications, and other latency sensitive industries. Multi access Edge Computing (MEC) is the foundation for embedding lightweight smart agents that facilitate closed-loop orchestration at the edge of the network. Such platforms reduce backhaul dependence and ensure service continuity during core outages, link degradation, and, overall, QoS/QoE provisioning. Edge based AI agents utilize continuous telemetry and contextual information and detect traffic anomalies within resource and operational bounds. Systemic, explainable, and robust AI closes the audit and resiliency gaps related to distributional shifts and adversarial attacks. Edge policy enforcement is assisted, and even rehearsed, through digital twin techniques [48], [70].

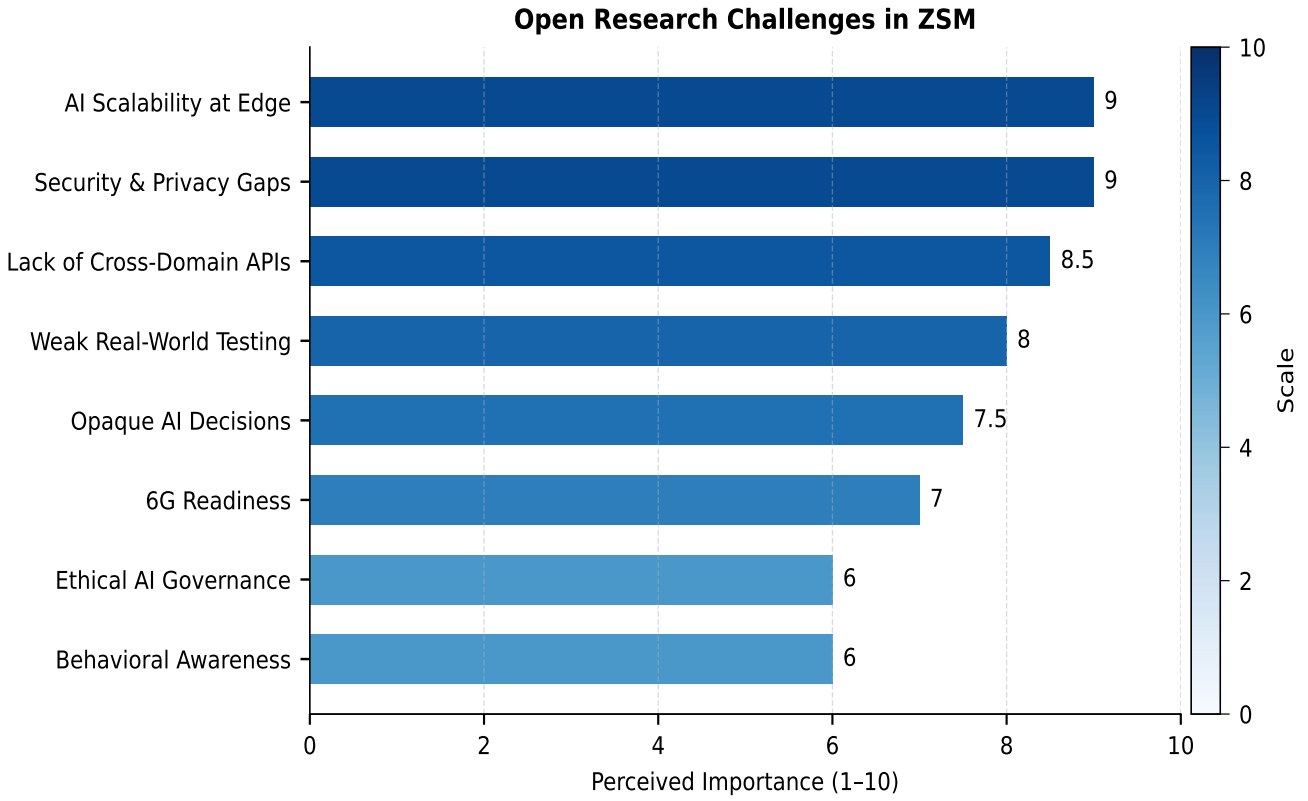

Fig. 9: ZSM Open Research Challenges, including scalability, explainability, cross-domain orchestration, and secure edge analytics.

Key components of edge-enabled ZSM

a) ***Stream Processing Engines****:* Low-latency analytics on live telemetry feeds (per-slice KPIs, RAN counters) to trigger micro reconfigurations which involves crowd-assisted signals can enrich observability [50], [73].

b) ***On Device Inference Models****:* Compressed, quantized, and pruned models for gateways and MEC servers(RL-driven prioritization and microservices-native VNFs support real time decisions) [41], [51], [54].

c) ***Federated Edge Intelligence****:* Collaborative learning across edge nodes without sharing raw data, including split learning, poisoning-resilient pipelines, and trustworthy FL tailored for ZSM [60].

- **Challenge:Computing limits at the edge**
  Solution: Hardware-accelerated edge (GPU/NPU), model compression/distillation, RL-guided service prioritization, and energy-aware scheduling for industrial workloads [15], [60].
- **Challenge:Inconsistent or sparse telemetry across nodes**
  Solution: Adaptive sampling, multi-source telemetry fusion, and slice-aware analytics pipelines integrated with ZSM orchestrators [50], [73].
- **Challenge:Security risks from physically exposed edge nodes and adversarial ML**
  Solution: Zero-trust controls with privacy-preserving credentials, FL defenses against poisoning, anomaly-aware micro-segmentation, and robust/XAI policies for trustworthy decisions [2], [77].
- **Challenge:Model drift and non-stationary traffic**
  Solution: Continuous evaluation and drift-aware switching at the edge, supported by digital twin-based A/B testing [82].

5) ***AI Hybrid and Multi-Model Approaches***

Hybrid AI architectures are increasingly adopted in ZSM to exploit complementary strengths across multiple learning paradigms. By combining supervised, unsupervised, and reinforcement learning, hybrid systems can both generalize from known patterns and adapt to novel, unlabeled conditions in cross-domain orchestration [73]. Supervised models forecast demand and congestion, while RL (e.g., DDPG, PPO, DQN families) reallocates resources under dynamic environments. This synergy enhances accuracy, adaptability, and policy robustness for zero-touch control loops [73].

- **Lifecycle management of slices** (placement, scaling, healing) [73], [75].
- **Proactive SLA violation prediction** and QoE-aware prioritization at cloud-native VNFs [41], [54].
- **Cross-domain policy reconciliation and orchestration** across RAN, edge, core, and vertical domains [73].

Recent developments also explore quantum inspired and fuzzy reasoning for uncertainty handling, alongside neuro

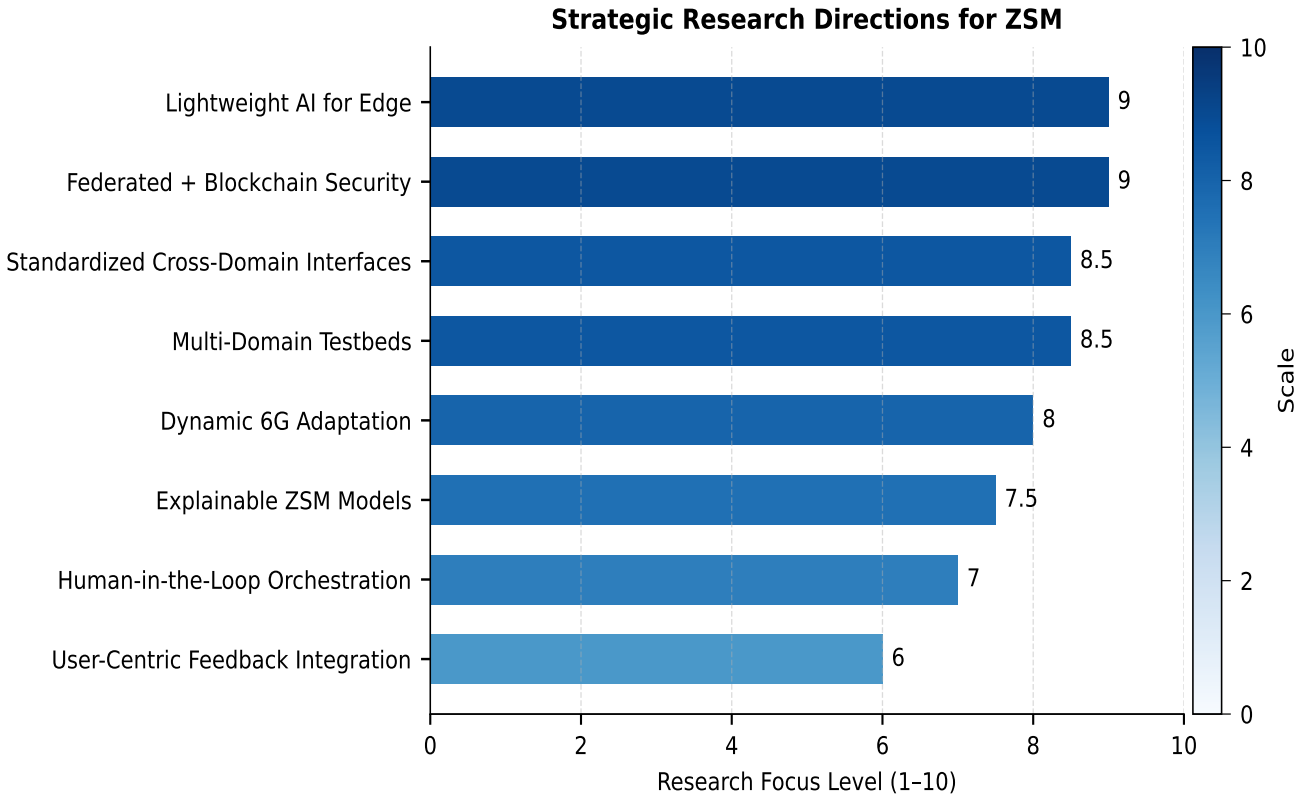

Fig. 10: ZSM Future Directions: edge intelligence, agentic AI, digital twins, and quantum-secure orchestration.

symbolic and XAI-driven hybrids that improve auditability and resilience [48], [86]. Such models are beneficial under partial observability and imprecise telemetry, conditions frequently encountered in multi domain ZSM.

Barriers and Research Opportunities

- **Integration Complexity:** Multi-model coordination requires consistent state sharing, conflict resolution, and composable policies across domains [1], [31], [56], [73].
- **Algorithmic Overhead:** Hybrid systems increase compute and latency; efficient scheduling, model selection, and RL-driven prioritization at the edge are needed [6], [41], [54].
- **Trust and Explainability:** As hybrid pipelines grow in complexity, embedded XAI and robust ML are essential for verifiable decisions, drift resilience, and operator trust [80], [82], [86].

The ZSM platforms will systemically depend on adaptive model orchestration layers that switch learning paradigms fit to context, resources, and service criticality. This will function with lifecycle governance for trusted AI (evaluation, retraining, rollback) and autonomy in automation in O-RAN/edge environments [89], [92].

*6) **Standardization Issues in Different Domains***

Achieving Zero-Touch Network and Service Management at scale requires considerable standardization on interfaces, data models, and orchestration semantics. Considered ZSM implementations are still domain-specific with most features remaining vendor proprietary and thereby compromising end-to-end service continuity in heterogeneous environments [1], [7], [56]. Cross-domain interoperability requires standardized APIs, service descriptors, and metadata schemas. Furthermore, unified information models must address and contain intent, lifecycle, and telemetry over RAN, core, edge, and third-party instruments consistently [31], [73].

Challenges and Bottlenecks:

- **Network Function Heterogeneity:** Some vendors provide closed zeros interfaces for NFV and orchestration which hampers automation and portability [10], [55], [56].
- **Siloed Lifecycle Management:** Per domain orchestration segments SLA enforcement, which disintegrates service assurance across slices and providers [73].
- **Disunited Intent Interpretation:** Although intent models are evolving within the levels, the semantics and assurance hooks remain inconsistent across the levels [92].

Promising Solutions:

- **Intent-Based Networking (IBN):** Transforms operator objectives into executed policies using AI/ML and assurance [13], [25].

- **Federated Service Orchestration:** Cross-domain federation is built for effortless handoff, service migration, and trust negotiation while maintaining operator autonomy [20], [73].
- **Model-Driven Automation:** Employs YANG/TOSCA style descriptors across the RAN edge core environments for validation, portability, and conformance [31], [73].
- **Agentic AI Integration:** Propositions for LLM and agent-driven orchestration [97], [99], [113], [113] positioned as adjuncts for legacy APIs, delivering semantic interoperability across disparate domains.

In 6G networks, as infrastructures become open, programmable, and O-RAN native, the need for cross-domain ZSM standardization becomes more important than ever. Without alignment, operators become inefficient, expose themselves to security threats, and face vendor lock-in [81]. ZSM deployments in trusted contexts will need cross-organization collaborations involving open-source communities, and industry associations under frameworks based on zero-trust and privacy preserving credentials.

Numerous challenges outlined previously should be viewed as systemic issues rather than merely technical challenges. In this regard, failures in establishing semantic interoperability are more a consequence of a lack of coordination and governance across the ecosystem than the immaturity of algorithms. Concerns about lightweight AI are about more than the computational efficiency of algorithms, they also relate to the expected sustainability of 6G networks, which aim to decrease the operational emissions of the networks to zero. The increase in publications related to ZSM and Agentic AI is not matched by a suitable scale of testbed validation, which gives rise to a crisis of reproducibility. Such gaps are manifest in RAN automation and NTNs in those domains, the orchestration frameworks are still largely simulation driven rather than tested and validated in real environments. Future work in this area will need to shift focus in developing frameworks in isolation toward providing systems that are verifiable, energy aware, and cross domain validated, while also addressing requirements in governance and sustainability.

III. ZSM Use Cases and Applications

Zero-Touch Network and Service Management (ZSM) has matured from a concept to a practical means of enabling self-driving 5G and 6G networks. ZSM enables self-configuration, self-optimization, self-healing, and self-protection in diverse environments by eliminating all manual configuration and intervention. This section describes the primary use cases and real-world deployments of ZSM across several industries, aligned where appropriate to the challenge areas.

A. Telecom Operations and Service Lifecycle

With ZSM, ZSM in telecommunications equips full end-to-end service lifecycle management. ZSM Enables full end-to-end service lifecycle management. Public cloud networks can be automated provisioned, monitored, scaled, and terminated in an automated fashion through closed-loop SLA and AI AI SLA enforcement, and closed loop SLA policing management [1], [4], [20]. This specifically falls under Real-World Validation, focusing on empirical feasibility and ZSM automated automotive highways in the trial. This specifically falls under Real World Validation focusing on empirical automotive trials feasibility and exhibits a number of automotive trials scalability and ZSM scalability bottlenecks.

B. Intent-Based Networking

With the emergence of intent-based networking, ZSM converts abstract operational or organizational objectives to practical network configurations. This alleviates the complexity of policy enforcement, limits manual mistakes, and speeds up the provisioning time of tailored services [9], [13], [25].

C. Network Slicing and RAN Automation

ZSM facilitate the automated creation and tailoring of separate virtual slices for various use cases for eMBB, URLLC, and mMTC sliced networks. In the RAN/O-RAN domain, ZSM engages with AI resource allocation, xApps/rApps, Digital Twins for real-time optimization, and ZSM [23], [31], [67], [70], [81].

D. Security and Privacy Orchestration

Alongside other benefits, ZSM frameworks are leveraged for maintaining real-time intrusion detection and response to multifaceted policies within AI-augmented networks for the purpose of privacy preservation and zero-trust security [2], [11], [12], [19], [77], [79].

E. Applications Specific to Each Vertical

The ZSM impact goes beyond telecom operations:

- **Autonomous transportation:** In Real World Validation of C-V2X, orchestration of movement of vehicles and smart highway zero touch orchestration [17], [91].
- **Healthcare and Tactile Internet:** URLLC enabled remote telemedicine and surgery, and haptic communication as outlined in 6G Use Case Readiness.
- **Industrial Internet of Things (IIoT):** Automation of smart factory systems, and provisioning of M2M systems [42], [51], [85].
- **Non-terrestrial Networks (NTN):** In Cross Domain Orchestration zero touch orchestrated UAV and satellite services, AI resource used [32], [35], [42], [83].
- **Enterprise Automation:** ZSM orchestrated OSS/BSS driven billing, invoicing and IT service management of supras [41], [55], [61].

Research works ([97], [99], [113]) demonstrates the potential impact of Agentic AI and the LLM-driven orchestration which enables real-time intent reaction, ease-of-use governance, and semantic interopability on the evolution

of the aforementioned use cases. These approaches will be accelerated in due time, as the convergence of normalization activities will be integrated to the evolution of ZSM to dependable cross-domain and 6G sustainable cross-domain sustainable deployments.

IV. Discussion and Research Gaps

This part of the text combines the gaps identified in the literature. It outlines unresolved issues and potential areas for new studies. Although great strides have been made in Zero-Touch Network and Service Management, issues remain which, if unresolved, will impede the achievement of the desired outcome of this study, the Intelligently Automated, Secure, and Scalable Network for the Next Generation of 6G and Beyond.

In the domain of literature for Zero-Touch Network and Service Management, work has been done in orchestration and the intergration of AI and security systems. However, there are still gaps in the literature which curb the development of Autonomous, Secure, Scalable Network Management System for 5G/6G. This is demonstrated in Table XVII, where the references from this study are used to highlight these gaps.

A. Architectural Gaps

ZSM frameworks [1], [4], [10] have been suggested modularly and along the lines of ETSI standards, however, the actual implementation of these frameworks remains sophisticated and immature in fully operational multi domain settings. Currently, the majority of implementations are constrained to computer generated simulations, laboratory environments, and domain capturing proofs of concept which are incredibly restrictive in terms of generalizability. This has the consequence of performance metrics, along with their critical components, being under evaluated in systems designed to scale optimally. O-RAN, along with other initiatives, seeks the unabated articulation of RAN with RAN control along with programmable access which, in turn, paves the way for vendors with minimal verification steps accessible [67], [81].

Most Important Limitations on Architecture:

- **End-to-End Interoperability:** Telemetry collectors, AI engines on policies, and orchestrators remain domain-specific, stifling cross-administrative interoperability [1], [31], [73].
- **Benchmarking Deficits:** There is no renowned, benchmark suite and reference implementation on ZSM evaluation for real world condition assessment. There is a dearth of open, comparable metrics, and reproducible testbeds [53], [56], [73], [75].
- **Challenges of Integrating Legacies:** There is a low level of compatibility with OSS/BSS systems. The middleware interface is frequently proprietary, ad hoc, or poorly designed [56].
- **ROI Models Remain Ambiguous Unclear Models:** Very few works quantify the OPEX–CAPEX trade offs of the automation, hence slowing down the adoption rate by operators due to economic constraints [53].

Research Directions and Solution Approach:

- **Open Reference Testbeds:** Extend multi domain testbeds and disseminate reproducible benchmarks for ZSM (E2E slicing, orchestration, assurance), in step with global 6G initiatives and O-RAN activities [53], [67], [75], [81].
- **Vendor Neutral Middleware:** Define and document OSS/BSS integration modules driven by model APIs (e.g., TMF Open APIs, YANG, TOSCA) aligned with ZSM reference architectures [31], [56], [73].
- **Digital Twin Validation:** Use network digital twins for rehearsals before the actual deployments of policy packs, SLA stress tests, and cost performance modeling across RAN edge core NTN domains [69], [70].
- **Hybrid Co-existence Frameworks:** Incorporate RL for service-level decision making and energy efficient scheduling within phased transition strategies that integrate bounded (deterministic) and learning (adaptive) control loops [51], [54].

Forthcoming efforts ought to shift toward large scale, integrative, and cost performance balanced architectures to resolve the dichotomy between conceptions and reality. Otherwise, the ZSM will remain as unfulfilled aspirations hovering above the 6G networks, and not as proper, deployable standards.

B. AI and Automation Gaps

AI provides a foundational capability in ZSM for autonomous orchestration, closed-loop adaptive control, and dynamic assurance. Yet, there are substantial architectural and operational challenges in production deployments. RL, Auto ML, and FL have been shown to have promise [3], [5], [6], but their effectiveness in real-world 5G/6G scenarios in terms of scalability and robustness. These gaps, shown in Table XVII, truly limit the maturity of network automation using AI.

Artificial Intelligence Techniques Limitations:

- **Time Spent Training:** Much of the RL implementations converge exceedingly slowly and need to spend many orders of interaction at cross purposes to time-sensitive service operations [54].
- **Heavy Optimization Cost:** The compute and energy costs of edge devices are derisively low, such that AutoML and FL spend too much time optimizing iterations of under [60].
- **Opaque:** The original Deep Orchestration agents design and architecture makes it hard to understand their

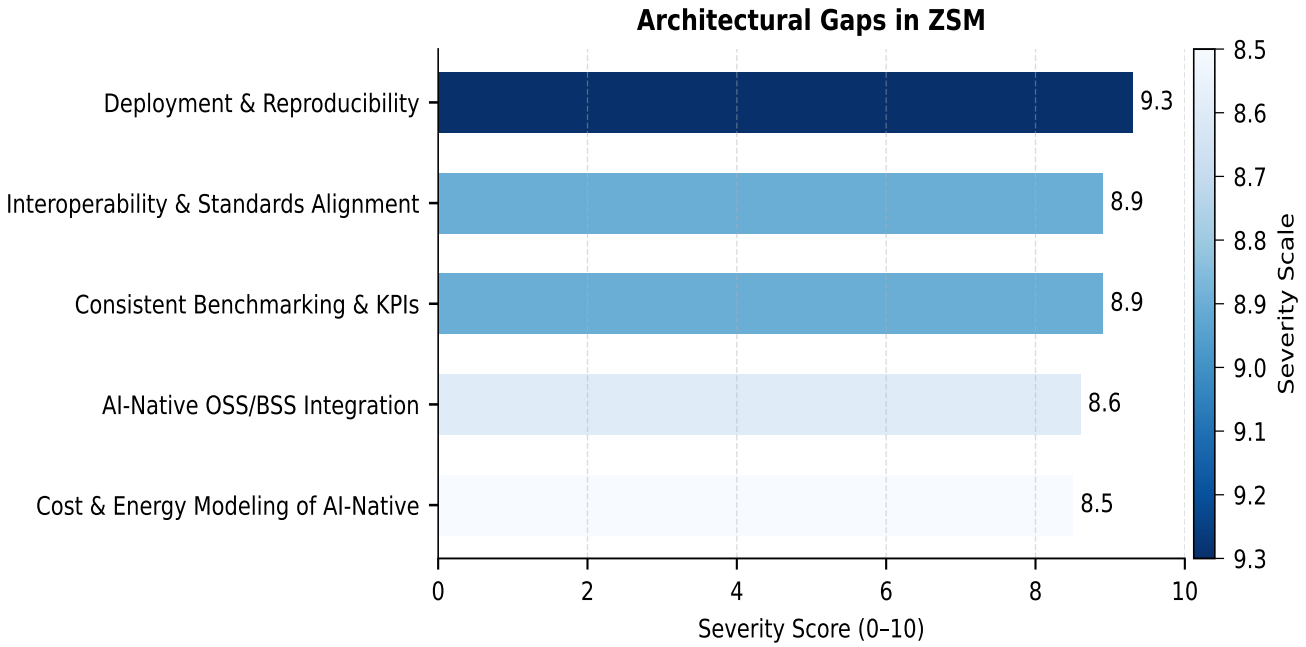

Fig. 11: Architectural gaps in ZSM.

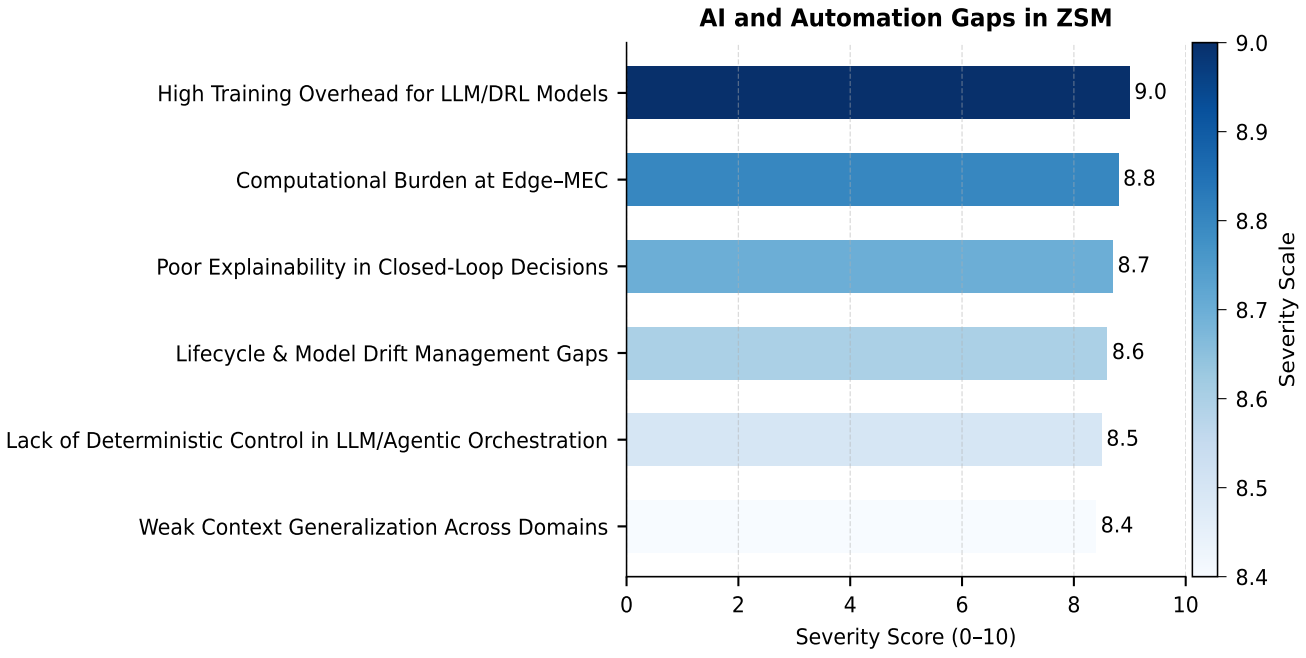

Fig. 12: AI and Automation Gaps in ZSM Standardization.

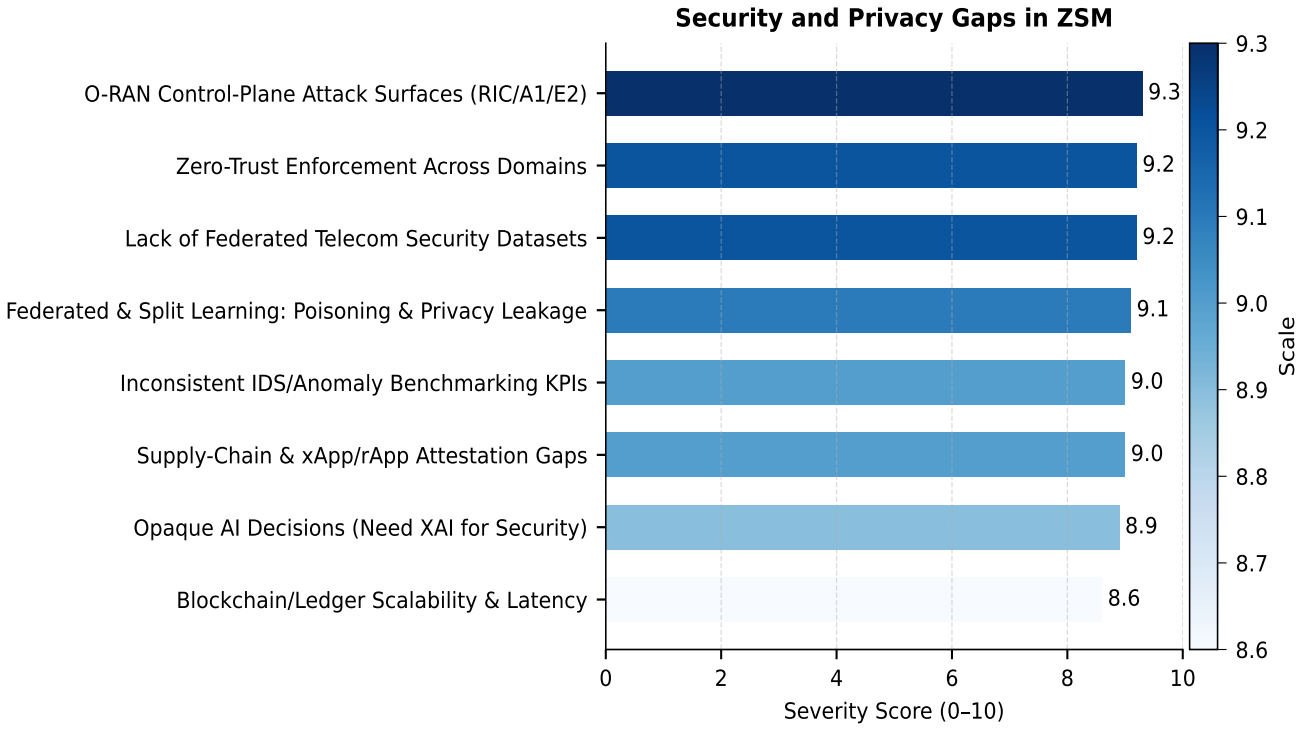

Fig. 13: Security and Privacy Gaps.

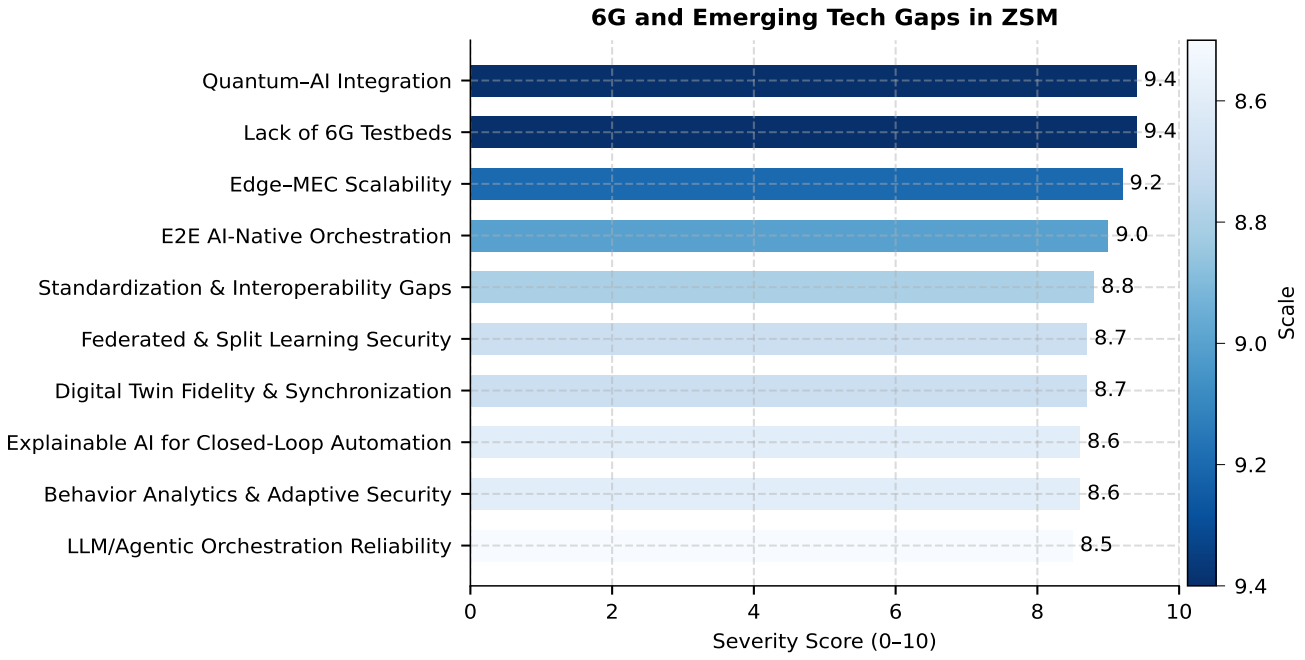

Fig. 14: Gaps in 6G and Emerging Technologies.

TABLE XVII Detailed Research Gaps and Directions Across ZSM Themes

References	Theme	Specific Gap	Evidence in the Cited Works	Promising Research Directions
[1], [4], [56], [110]	ZSM Architecture	Few vendor-neutral, cross-domain pilots with standardized KPIs/telemetry; lack of reproducible testbeds and open benchmarks.	[1] ZTM across ETSI/NFV/SDN interoperability/testability challenges. [4] Experimental ZTM/M&O missing common metrics. [56] Evolutionary 6G view calls for scalability and comparability. [110] Recent 6G validation study emphasizes reference testbeds.	• Open E2E reference stacks with *public* KPIs/data schemas. • Cross-vendor pilots using identical descriptors/telemetry feeds. • Community benchmarks and CI pipelines for ZSM regressions.
[6], [54], [86], [113]	AI in ZSM	Need real-time, explainable, low-latency AI at the edge; weak scheduling/prioritization for VNFs; limited drift/robustness handling in loops.	[6] Closed control loops timeliness/coordination constraints. [54] DDPG-based VNF scheduling anti-starvation challenges. [86] XAI in O-RAN operator trust and explainability. [113] Recent OSS-GPT work early signs of LLM-assisted orchestration.	• Edge-amenable models with latency SLAs. • Multi-objective schedulers (QoS/energy/reliability). • Drift-aware monitoring with safe rollback.
[2], [8], [62], [117]	Security & Privacy	Operationalizing Zero-Trust, FL and privacy credentials at scale; need poisoning/Byzantine-resilient pipelines and auditable policies.	[2] ZTA patterns for 5G+ (continuous verification). [8] FL defenses against poisoning in constrained ZTM. [62] Attribute-based credentials for privacy-preserving orchestration. [117] O-RAN threat model study new empirical validation gaps.	• End-to-end ZT enforcement across RAN–core–edge. • Robust FL (Byzantine tolerance, secure aggregation). • Credential lifecycle integrated with orchestrators.
[13], [31], [75], [114]	Service Lifecycle	No unified slice/service descriptors and cross-domain APIs with harmonized intent semantics; fragmented assurance across providers.	[13] Intent-driven pipelines shared semantics missing. [31] 6G slice M&O with domain managers coordination gaps. [75] End-to-end slicing architecture open but fragmented. [114] Survey on intent-based orchestration portability still weak.	• ETSI/3GPP-aligned descriptors + TMF APIs. • Intent ontologies mapped to policies/SLAs. • Cross-domain assurance with common telemetry contracts.
[52], [70], [83], [123]	Future Technologies	6G scenarios (tactile/holographic, O-RAN-native, LEO/NTN) lack empirical validation and latency-aware orchestration models; limited DT-based closed-loop tests.	[52] Tactile Internet orchestration requirements. [70] Digital twins for O-RAN rollback/safety mechanisms. [83] AI for satellite/NTN orchestration dynamic challenges. [123] New study on 6G digital twins synchronization gaps.	• Digital-twin-in-the-loop evaluations for O-RAN/LEO orchestration. • Heterogeneous E2E controllers aware of NTN dynamics. • Field trials with shared traces for replicability.

workings. This fosters a lack of sufficient belief supporting high levels of trust necessary for dependability, verification of SLAs, and the compliance to rigid control frameworks of the operators managing such infrastructures [57], [80], [86].

- **Context Drift and Generalization:** There are issues like heterogeneity, drift in data, and telemetry that is non-IID across multiple slices or domains, which greatly leads to degradation of the models [76], [82].
- **Low Degree of Development:** There are OSS-GPT that shows promise for LLM assisted orchestration [113] but the benchmarks, safety and constrain latency, remain to be developed further.

Research Directions and Solutions:

- **Lightweight AI Models:** Pruning, quantization, and knowledge distillation for edge-friendly agents; RL-based service prioritization and energy-aware scheduling tailored to 6G SLAs [51], [54].
- **Explainable AI Integration:** Embedding SLA- and policy-aware explainability into orchestration loops

(e.g., XAI modules for O-RAN and slicing) to improve operator trust and accountability [57], [80], [86].
- **Meta-Learning Approaches:** Accelerating adaptation to new domains through few-shot learning and transfer learning to mitigate drift and heterogeneity [76].
- **Collaborative Learning Frameworks:** Split learning and federated learning with poisoning resilience, privacy-preserving aggregation, and continual retraining to handle diverse edge data sources [29], [60], [88].
- **Agentic and LLM-Assisted Control:** Benchmarking safety, latency, and energy trade-offs of large language models in orchestrator loops (e.g., OSS-GPT and related frameworks) [113].

Key Use Cases for Lightweight, Interpretable AI in ZSM: Resource multiplexing in V2X and self-driving ecosystems with ultra-low latency. Industrial IoT Fault Prediction: Anomaly recovery and real time detection in critical operational networks. Dynamic SLA Assurance: Resource allocation for bounded 5G/6G slices with asynchronous QoS/QoE guaranteed [51], [54], [85]. Agentic O-RAN Control: Usage of LLM enabled controllers for negotiation, supervision, and orchestration reasoning in open RAN [113].

C. Security and Privacy Gaps

ZSM is designed and deployed on the premise that there is sufficient security and privacy and while novel approaches exist, very little is done to scientifically validate them which is very unfortunate. Where decentralization and elasticity is a must, alongside trustless frameworks and ZTA paradigms, the trust model remains tethered to a primitive architectural stage. The underexposed leaps that need to be conquered still depend on the answers to questions like network fragments, consensus holdups, or even denial and informations systems attacks [65], [77]. The same establishes for privacy-preserving Tier 1 orchestration credentials and the need to aggregation the primitive level of common reputation systems and uniform metric evaluations across domains [62], [64]. The FL frameworks embedded in the IDS architecture still remain foreign to datasets and class perturbation frameworks, resulting in isolatable inflexibility across analysis [88].

Understanding these finite gaps in explainability is just as perplexing. The lack of transparency on the justifications on the outcomes from the core of the agility mesh fabric such as the zero height boundaries, and the adaptive 5D sight engines, undermines system trust. In addition, the evolving edges of Zero Touch and Zero Trust as the limbs of convergence, increase the rate of collision for the design of orchestration and security co-design. Automation distributed on the edge systems through fine microns can be enhanced for system control through dense, aggregated clusters in a unified orchestration zone with Zero Control [77], [79]. The table simplifies these overlapping challenges in evidence and documents the research directions of gaps in the defense systems for ZSM aligned with the proof of Table XVII.

Key Limitations:

- **Multi-Domain Scalability:** The latency, partitioning, and consensus delays with blockchain and ZTA-based trust models in distributed ZSM [65], [77].
- **Absence of Standardized Datasets:** Common evaluation suites for FL-based IDS and poisoning defense methods are non-existent and, therefore, reproducibility is stifled [88].
- **Limited Explainability:** The majority of security analytics do not incorporate SLA or context aware explanations, which diminishes trust from operators [80], [86].

D. Service Lifecycle Gaps

The continued lack of service lifecycle automation across different layers, vendors, and domains leads to fragmented service lifecycle automation and inhibits seamless end-to-end orchestration in 5G and beyond. While intent-based networking has been extensively promoted [7], [13], [30], contemporary orchestrators still do not share domain semantics and state visibility. This results in inconsistent enforcement, unresponsiveness to rapid scaling during mobility, and service descriptors portability issues [79], [92]. Furthermore, legacy OSS/BSS systems still create bottlenecks with proprietary interfaces and an absence of model-driven descriptors [56]. Additional ZSM lifecycle verification in ZTA increases overhead in MEC, UAV, and LEO domains, straining existing models [77], [79]. The literature illustrates these limitations, which are discussed in more detail in Table XVII. For instance, studies on intent-driven orchestration pipelines [13] discuss the lack of shared semantics, and multi-domain slice management frameworks [31] discuss gaps in cross-domain coordination. Studies on intelligent slicing [75], [114] state that although open APIs exist, they are too fragmented and lack interoperability between providers to allow for widespread automation. More recent studies on intent-based closed-loop orchestration [120] and programmable service lifecycle platforms [122] argue the importance of having standardization and descriptors that allow for automation.

Key Limitations in Service Lifecycle Management:

- **Integrated Service and Slice Descriptors:** Writings on cohesion gaps on tailored service and slice descriptors that concern ETSI/3GPP specifications and barriers to interoperability [13], [75], [120].
- **Weak Cross-Domain Assurance:** Self-contained service level assurance (assurance silos) is prevalent, because orchestrators do not furnish state reconciliation and SLA enforcement mechanisms, across multiple providers [31], [79], [122].
- **Legacy System Bottlenecks:** Due to proprietary OSS/BSS interfaces, ease of integration and automation limits, still underpin the silos [56].

- **Overhead Security Clause in Lifecycle Events:** The fragmentation of ZTA enforcement, exacerbated by on-distributed verification in MEC/UAV/LEO cases, is a distributed concern for ZSM lifecycle verification [77], [79], [117].

Strategic Research Directions:

- **Unified Intent Ontologies:** Partnership with SDOs in developing portable semantics for vendor and domain silo cross-orchestration [92], [120].
- **Cross-Domain State Reconciliation:** For SLA proof and distributed assurance, evidence consistent SLA cross-domain and distributed assurance with light ledgers and gossip architecture implementations [64], [77], [79], [122].
- **Interoperable Middleware:** To connect OSS/BSS in the ZSM domain, use TMF Open APIs and model driven standards (YANG/TOSCA) to the legacy OSS/BSS and open APIs [56].
- **Incorporating ZTA elements of security into monitored and verified lifecycles:** ZTA should be implemented as a lifecycle element for continuous verification, with fine-grained access control, for adaptive recovery and augmentative applications [77], [79], [117].

In summary, ZSM cycle automation is still very fragmented and blind to security in most areas. As highlighted in Table XVII, in order to support vz 6G networks, we need to advance to unified descriptors, portable intent semantics, and automated security orchestration which is essential for cross-domain, service, and lifecycle management.

E. Gaps in 6G and Emerging Technologies

The 6G roadmap anticipates tactile internet and holographic communications, as well as AI-native networking and NTN/aerial integration [22], [52], [78]. Nonetheless, as underscored, large-scale heterogeneous testbeds and emulation environments continue to be limited. This hinders the empirical validation of orchestration blueprints. With respect to digital twins, recent works [69], [70], [123] highlights their potential regarding safe rollback and predictive orchestration, yet implementations to date remain conceptual or confined to simulation. Zero Trust and Zero Touch integration still need to demonstrate their horizontal scalability across MEC, UAVs, and LEO constellations under bursty distributed traffic [32], [35], [77], [79]. The absence of behavioral and human-centric orchestration is another open challenge. User-centric research [15], [66] explores the impact of QoE and sentiment-driven policies, but ZSM frameworks still lack behavioral analytics in intent subsumption and closed-loop automation. This results in responsiveness gaps in public safety, emergency response, and immersive XR, which rely on adaptive systems as fundamental. Research in Quantum–AI is still at the nascent phase, but some recent surveys [65], [78] and frameworks [105] point to areas where secure orchestration and hybrid optimization might be potential focuses. The NISQ-era error-bounded problem, post-quantum cryptography, and ZTA-driven trust anchors Table III still remain unresolved.

At last, the onset of agentic AI poses both new opportunities and new challenges.

Initial research focuses on utilizing large language models for intent management [92], [113], [115], agent-based orchestration within the edge cloud continuum [97], [99], the hierarchical control of RANs [100], and employing foundational models as orchestration agents [98], [106], [107]. Further developments include agent marketplaces and observability frameworks [101], [102]. Nevertheless, considerable gaps still exist in the areas of safety, verification, benchmarking, operator-in-the-loop governance, and, arguably most importantly, the overarching frameworks necessary for practical implementation Table IV–VIII). Although complementary forecasting and orchestration studies [93]–[96] provide necessary components, they curiously refrain from the establishment of auditable agent societies, leaving a critical gap.

Future Innovation Pathways:

- **Behavior Aware ZSM Frameworks:** Context- and sentiment-driven orchestration policies for mission-critical services (e.g., XR, tactile internet) [15], [66].
- **Quantum AI Co Design:** Hybrid optimization and QML approaches for secure, autonomous orchestration with quantum-safe anchors [65], [78], [105].
- **Scalable Edge NTN Coordination:** Multi-agent RL and federated control for low-latency, resilient orchestration across MEC, UAV swarms, and LEO satellites [32], [35], [77], [79].
- **Digital-Twin Driven Validation:** High-fidelity digital twins integrated with orchestration loops to support reproducible testing and safe rollback in dynamic 6G scenarios [69], [70], [123].
- **Agentic AI for ZSM:** Reasoning-driven agents (LLM augmented or RL based) for intent negotiation, service assurance, and self-healing. Future work must emphasize safety, governance, and standard benchmarking [92], [95], [107].

To conclude, the unification of human-aware policy integration, quantum-safe orchestration, scalable MEC-NTN synchronization, digital-twin verification, and reliable agentic AI into a singular ZSM framework is necessary to bridge these gaps.

V. CONCLUSION

This survey integrates foundational theory with practical architectural advancements to provide a consolidated overview of Zero Touch Network and Service Management in 6G. Based on 128 studies published between 2021 and 2025, it evaluates the state of intent driven orchestration, AI native automation, cross domain management, and trust control systems. The data asserts that concepts of ZSM

theory have developed, partially aided by the modular architecture of ETSI, cloud native service fabrics, O-This survey identifies a vital consideration pertaining to ZSM evolution; it is not a question of the availability of smart building blocks to the system, but rather tackling the disparate ecosystem within which the components reside. There is a lack of unity in intent representation languages across different administrative domains. Inoperability persists across multi domain orchestrators, and the available testbeds are insufficient in scale and diversity to enable meaningful evaluation. Other constraints stem from the complexity of real-time explanation of automated responses; lifecycle assurance across several domains, and safeguards to protect against federated intelligence poisoning. Integrating zero-trust frameworks and privacy-preserving techniques in dispersed systems also remains an issue. Even though a number of architectures incorporate promising design elements, the underlying concepts are often miniaturized to small scale, single domain experiments, and do not encompass the full scope of operational challenges presented by 6G automation.

RAN programmability, and AI driven closed loops. Nevertheless, there is still a lack of fully autonomous implementations in countless 6G deployments. The considerable theoretical development is yet to be incorporated into fully operational large-scale environments, thereby leading to a gap between expectations and actual deployment. This survey identifies a vital consideration pertaining to ZSM evolution; it is not a question of the availability of smart building blocks to the system, but rather tackling the disparate ecosystem within which the components reside. There is a lack of unity in intent representation languages across different administrative domains. Inoperability persists across multi domain orchestrators, and the available testbeds are insufficient in scale and diversity to enable meaningful evaluation. Other constraints stem from the complexity of real-time explanation of automated responses; lifecycle assurance across several domains, and safeguards to protect against federated intelligence poisoning. Integrating zero-trust frameworks and privacy-preserving techniques in dispersed systems also remains an issue. Even though a number of architectures incorporate promising design elements, the underlying concepts are often miniaturized to small scale, single domain experiments, and do not encompass the full scope of operational challenges presented by 6G automation.

This part describes the most important areas and issues in your future work. There is a lack of trust, representation and integration across domains, no independent control of the processes, accountability and explainability. There are no scalable and reproducible testbeds to permit meaningful experimentation across multiple operators. There is a tendency to treat some issues in isolation e.g. security, post-quantum protections, federated learning, and privacy rather than integrate them into a coherent whole. Also, there are gaps in the automation of on boarding, assurance, drift control, and verification of intent.

Feedback on the above issues is the starting point to propose a first draft of a roadmap in future 6G ZSM (Zero-touch Service Management) systems. To avoid gaps across domains and to enhance explainability, enforcement, and translation, we need standardized, semantic intent languages. For real-time execution, orchestration requires lightweight models of AI which are interpretable and work at the edge. Digital twins of O RAN, transport networks, and service fabrics provide environments for continuous assurance and safe evaluation. Privacy-preserving federated intelligence, for multi-operator systems, supportive of cooperative decision-making, must withstand poisoning attack scenarios. New Design for Zero Trust and Quantum Resiliency are a must for the high distributed 6G Architecture. Contextual adaptation and automation can be achieved with agent-based systems reinforced with structured workflows, feedback loops, and AI.

Overall, this work provides a unified taxonomy and comparative framework for the next generation of ZSM systems. It outlines the architectural, analytical, and governance principles needed to progress toward fully autonomous 6G networks. Future research and standardization activities are expected to build on these insights and accelerate industrial adoption. As 6G expands to support extended reality, autonomous and cognitive IoT applications, intelligent mobility, and healthcare, ZSM will play a central role. By enabling a resilient, flexible, and human centered operational model across heterogeneous aerial, terrestrial, and non terrestrial networks, ZSM will contribute strongly to the socio economic impact envisioned for next generation communication systems.

REFERENCES

[1] E. Coronado *et al.*, "Zero touch management: A survey of network automation solutions for 5g and 6g networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2535–2578, 2022.

[2] K. Sowjanya, D. Saha, and B. Lall, "Zero-trust security in 5g and beyond networks: An overview," in *2025 17th International Conference on COMmunication Systems and NETworks (COMSNETS)*. IEEE, Jan. 2025, pp. 1230–1234.

[3] F. Ahmed, M. Lee, S. Y. Lien, S. Subramaniam, M. Matsuura, H. Hasegawa, and S. C. Lin, "Federated deep reinforcement learning-driven o-ran for automatic multirobot reconfiguration," *arXiv preprint*, 2025.

[4] S. Barrachina-Muñoz, F. Rezazadeh, L. Blanco, S. Kukliński, E. Zeydan, A. Chawla, L. Zanzi, F. Devoti, V. Vlahodimitropoulou, I. Chochliouros, and A. M. Bosneag, "Empowering beyond 5g networks: An experimental assessment of zero-touch management and orchestration," *IEEE Access*, 2024.

[5] L. Yang, M. E. Rajab, A. Shami, and S. Muhaidat, "Enabling automl for zero-touch network security: Use-case driven analysis," *IEEE Transactions on Network and Service Management*, 2024.

[6] N. F. S. de Sousa, M. T. Islam, R. U. Mustafa, D. A. L. Perez, C. E. Rothenberg, and P. H. Gomes, "Machine learning-assisted closed-control loops for beyond 5g multi-domain zero-touch networks," *Journal of Network and Systems Management*, vol. 30, no. 3, p. 46, 2022.

[7] D. Giannopoulos, G. Katsikas, K. Trantzas, D. Klonidis, C. Tranoris, S. Denazis, L. Gifre, R. Vilalta, P. Alemany, R. Muñoz, and A. M. Bosneag, "Across: Automated zero-touch cross-layer provisioning framework for 5g and beyond vertical services," in *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, Jun. 2023, pp. 735–740.

[8] S. B. Saad, B. Brik, and A. Ksentini, "Toward securing federated learning against poisoning attacks in zero touch b5g networks," *IEEE Transactions on Network and Service Management*, vol. 20, no. 2, pp. 1612–1624, 2023.

[9] A. I. Manolopoulos, V. M. Alevizaki, M. Anastasopoulos, and A. Tzanakaki, "An ai-assisted framework for lifecycle management of beyond 5g services," *IEEE Access*, 2024.

[10] I. Ashraf, Y. B. Zikria, S. Garg, Y. Park, G. Kaddoum, and S. Singh, "Zero touch networks to realize virtualization: Opportunities, challenges, and future prospects," *IEEE Network*, vol. 36, no. 6, pp. 251–259, 2022.

[11] H. Byeon, M. Alsaadi, S. Gupta, J. C. Patni, T. A. Ahanger, B. K. Singh, A. K. Srivastava, P. S. Abdinabievna, and S. Boddupalli, "Zero trust management over consumer technology based iot edge node for sdn communication and control of cyber-physical systems," *IEEE Transactions on Consumer Electronics*, 2025.

[12] S. Batewela, P. Ranaweera, M. Liyanage, E. Zeydan, and M. Ylianttila, "Addressing security orchestration challenges in next-generation networks: A comprehensive overview," *IEEE Open Journal of the Computer Society*, 2025.

[13] Y. Wang, C. Yang, T. Li, Y. Ouyang, X. Mi, and Y. Song, "A survey on intent-driven end-to-end 6g mobile communication system," *IEEE Communications Surveys & Tutorials*, 2025.

[14] M. L. Gambo and A. Almulhem, "Zero trust architecture: A systematic literature review," 2025, preprint or Unpublished Work.

[15] K. B. Ajeyprasaath and P. Vetrivelan, "A hybrid machine learning approach for improvised qoe in video services over 5g wireless networks," *Computers, Materials & Continua*, vol. 78, no. 3, 2024.

[16] M. Ravi, T. A. Sheikh, and Y. Bulo, "Optimal resource allocation and data communication in 5g and beyond with a cell-free iots systems," 2024, unpublished or whitepaper.

[17] R. C. Bello, N. S. Kriještorac, M. Pokorn, J. Hribar, C. Fortuna, and J. M. Marquez-Barja, "Building zero-touch service management framework for automotive services using the smart highway testbed," in *2024 7th International Balkan Conference on Communications and Networking (BalkanCom)*. IEEE, Jun. 2024, pp. 212–217.

[18] S. B. Saad, B. Brik, and A. Ksentini, "A trust and explainable federated deep learning framework in zero touch b5g networks," in *GLOBECOM 2022 - IEEE Global Communications Conference*. Rio de Janeiro, Brazil: IEEE, 2022, pp. 1037–1042.

[19] S. Batewela, M. Liyanage, E. Zeydan, M. Ylianttila, and P. Ranaweera, "Security orchestration in 5g and beyond smart network technologies," *IEEE Open Journal of the Computer Society*, 2025.

[20] M. E. Rajab, L. Yang, and A. Shami, "Zero-touch networks: Towards next-generation network automation," *Computer Networks*, vol. 243, p. 110294, 2024.

[21] A. El Mettiti and M. Oumsis, "A survey on 6g networks: Vision, requirements, architecture, technologies and challenges," *Networks*, vol. 3, p. 4, 2022.

[22] S. N. Karahan, Yazici, Duru, and S. Çimen, "Ai-native use cases in 6g," in *2025 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA)*. IEEE, May 2025, pp. 1–9.

[23] S. Rani, H. Babbar, M. Krichen, K. Yu, and F. H. Memon, "Network slicing for zero-touch networks: A top-notch technology," *IEEE Network*, vol. 37, no. 5, pp. 16–24, 2023.

[24] S. Shakya, R. Abbas, and S. Maric, "A novel zero-touch, zero-trust, ai/ml enablement framework for iot network security," *arXiv preprint*, 2025.

[25] L. Velasco, M. Signorelli, O. G. D. Dios, C. Papagianni, R. Bifulco, J. J. V. Olmos, S. Pryor, G. Carrozzo, J. Schulz-Zander, M. Bennis, and R. Martinez, "End-to-end intent-based networking," *IEEE Communications Magazine*, vol. 59, no. 10, pp. 106–112, 2021.

[26] A. Bandi and S. Yalamarthi, "Towards artificial intelligence empowered security and privacy issues in 6g communications," in *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*. IEEE, Apr. 2022, pp. 372–378.

[27] Z. Li, Z. Li, X. Xiong, and D. Liu, "Cross-domain ai towards 6g: Requirements, solution, and validation," in *2024 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, May 2024, pp. 456–460.

[28] O. Iacoboaiea, J. Krolikowski, Z. B. Houidi, and D. Rossi, "From design to deployment of zero touch deep reinforcement learning wlans," *IEEE Communications Magazine*, vol. 61, no. 2, pp. 104–109, 2022.

[29] F. Naeem, M. Ali, and G. Kaddoum, "Federated-learning-empowered semi-supervised active learning framework for intrusion detection in zsm," *IEEE Communications Magazine*, vol. 61, no. 2, pp. 88–94, 2023.

[30] G. Samaras, V. Theodorou, D. Laskaratos, N. Psaromanolakis, M. Mertiri, and A. Valantasis, "Qmp: A cloud-native mlops automation platform for zero-touch service assurance in 5g systems," in *2022 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*. IEEE, Sep. 2022, pp. 86–89.

[31] H. Chergui, A. Ksentini, L. Blanco, and C. Verikoukis, "Toward zero-touch management and orchestration of massive deployment of network slices in 6g," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 86–93, 2022.

[32] C. Grasso, R. Raftopoulos, and G. Schembra, "Smart zero-touch management of uav-based edge network," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 4350–4368, 2022.

[33] E. Baccour, M. S. Allahham, A. Erbad, A. Mohamed, A. R. Hussein, and M. Hamdi, "Zero touch realization of pervasive artificial intelligence as a service in 6g networks," *IEEE Communications Magazine*, vol. 61, no. 2, pp. 110–116, 2023.

[34] A. Mekrache, M. Mekki, A. Ksentini, B. Brik, and C. Verikoukis, "On combining xai and llms for trustworthy zero-touch network and service management in 6g," *IEEE Communications Magazine*, 2024.

[35] A. Galli, P. G. Giardina, M. Guta, L. Lossi, A. Mancina, V. Moscato, F. Patrone, C. Roseti, S. P. Romano, G. Sperlí, and F. Zampognaro, "Ai for zero-touch management of satellite networks in b5g and 6g infrastructures," in *AI6G@WCCI*, 2022.

[36] S. Wang, M. A. Qureshi, L. Miralles-Pechuán, T. Huynh-The, T. R. Gadekallu, and M. Liyanage, "Explainable ai for 6g use cases: Technical aspects and research challenges," *IEEE Open Journal of the Communications Society*, 2024.

[37] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open ran security: Challenges and opportunities," *Journal of Network and Computer Applications*, vol. 214, p. 103621, 2023.

[38] C. Trivedi, P. Bhattacharya, V. K. Prasad, V. Patel, A. Singh, S. Tanwar, R. Sharma, S. Aluvala, G. Pau, and G. Sharma, "Explainable ai for industry 5.0: Vision, architecture, and potential directions," *IEEE Open Journal of Industry Applications*, 2024.

[39] E. E. Seder, G. Bernini, M. Iordache, R. Mihai, J. Brenes, C. Patachia, C. Brezeanu, M. Ruta, and G. Landi, "Ai-driven zero-touch slice optimization for 6g networks," in *2024 IEEE 29th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, Oct. 2024, pp. 1–6.

[40] H. H. H. Mahmoud, A. A. Amer, and T. Ismail, "6G: A comprehensive survey on technologies, applications, challenges, and research problems," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, p. e4233, 2021.

[41] S. B. Chetty, A. Nag, A. Al-Tahmeesschi, Q. Wang, B. Canberk, J. Marquez-Barja, and H. Ahmadi, "Optimized resource allocation for cloud-native 6g networks: Zero-touch ml models in microservices-based vnf deployments," *IEEE Network*, 2024.

[42] Z. A. E. Houda, B. Brik, and A. Ksentini, "Securing iiot applications in 6g and beyond using adaptive ensemble learning and zero-touch multi-resource provisioning," *Computer Communications*, vol. 216, pp. 260–273, 2024.

[43] A. Rizwan, M. Jaber, F. Filali, A. Imran, and A. Abu-Dayya, "A zero-touch network service management approach using ai-enabled cdr analysis," *IEEE Access*, vol. 9, pp. 157 699–157 714, 2021.

[44] I. A. Ridhawi, M. Aloqaily, F. Karray, M. Guizani, and M. Debbah, "Realizing the tactile internet through intelligent zero touch networks," *IEEE Network*, 2022.

[45] K. Abbas, Y. Cho, M. Afaq, A. Nauman, J. H. Yoo, J. W. K. Hong, and W. C. Song, "Ibn-ztsa: Ai-ibn for zero touch service automation of b5g terrestrial and non-terrestrial networks," *IEEE Communications Standards Magazine*, 2025.

[46] W. B. Abbas, Q. Z. Ahmed, F. A. Khan, N. S. Mian, P. I. Lazaridis, and P. Sureephong, "Designing future wireless networks (fwns) with net zero (nz) and zero touch (zt) perspective," *IEEE Access*, vol. 11, pp. 83 301–83 321, 2023.

[47] S. Roy, H. Chergui, and C. Verikoukis, "Tefl: Turbo explainable federated learning for 6g trustworthy zero-touch network slicing," *arXiv preprint*, 2022.

[48] M. S. Munir, K. T. Kim, A. Adhikary, W. Saad, S. Shetty, S. B. Park, and C. S. Hong, "Neuro-symbolic explainable artificial intelligence twin for zero-touch ioe in wireless network," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 22 451–22 468, 2023.

[49] M. Gupta, R. K. Jha, and S. Jain, "Tactile based intelligence touch technology in iot configured wcn in b5g/6g - a survey," *IEEE Access*, vol. 11, pp. 30 639–30 689, 2022.

[50] A. Tarrías, A. Moreno, F. Pareja, E. Baena, S. Fortes, and R. Barco, "Towards zero-touch cellular networks via next-generation crowdsourcing," *IEEE Access*, 2024.

[51] S. Prathiba, K. Raja, R. Saiabirami, and G. Kannan, "An energy-aware tailored resource management for cellular-based zero-touch deterministic industrial m2m networks," *IEEE Access*, 2024.

[52] Z. Hou, C. She, Y. Li, D. Niyato, M. Dohler, and B. Vucetic, "Intelligent communications for tactile internet in 6g: Requirements, technologies, and challenges," *IEEE Communications Magazine*, vol. 59, no. 12, pp. 82–88, 2022.

[53] D. Sabella, G. Nardini, P. Demestichas, S. Barmpounakis, D. Phan-Huy, M. Merluzzi, E. Gamazo, A. Ramos, G. Landi, M. Leinonen, and A. Pärssinen, "Innovation management in 6g research: the case of hexa-x project," *IEEE Communications Magazine*, vol. 62, no. 2, pp. 142–149, 2023.

[54] S. Chetty, H. Ahmadi, and A. Nag, "A ddpg-based zero-touch dynamic prioritization to address starvation of services for deploying microservices-based vnfs," *IEEE Transactions on Machine Learning in Communications and Networking*, 2024.

[55] A. Arulappan, G. Raja, K. Passi, and A. Mahanti, "Optimization of 5g/6g telecommunication infrastructure through an nfv-based element management system," *Symmetry*, vol. 14, no. 5, p. 978, 2022.

[56] G. Karam, M. Gruber, I. Adam, F. Boutigny, Y. Miche, and S. Mukherjee, "The evolution of networks and management in a 6g world: An inventor's view," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 5395–5407, 2022.

[57] N. Khan, S. Coleri, A. Abdallah, A. Celik, and A. Eltawil, "Explainable and robust artificial intelligence for trustworthy resource management in 6g networks," *IEEE Communications Magazine*, vol. 62, no. 4, pp. 50–56, 2023.

[58] M. Corici, F. Eichhorn, R. Bless, M. Gundall, D. Lindenschmitt, B. Bloessl, M. Petrova, L. Wimmer, R. Kreuch, T. Magedanz, and H. Schotten, "Organic 6g networks: Vision, requirements, and research approaches," *IEEE Access*, vol. 11, pp. 70 698–70 715, 2023.

[59] F. Luque-Schempp, L. Panizo, and P. Merino, "Automadapt: Zero touch configuration of 5g qos flows extended for time-sensitive networking," *IEEE Access*, vol. 11, pp. 82 960–82 977, 2023.

[60] H. Hafi, B. Brik, P. Frangoudis, A. Ksentini, and M. Bagaa, "Split federated learning for 6g enabled-networks: Requirements, challenges, and future directions," *IEEE Access*, vol. 12, pp. 9890–9930, 2024.

[61] M. Vivek and A. Chidambaram, "Implementation and benefits of zero-touch invoice processing in manufacturing industries," *Unpublished/Industry Report*, 2024.

[62] A. Kunz, R. Asensio-Garriga, J. Rodriguez, J. Bernabé, A. Gomez, S. Baskaran, and S. Paul, "Privacy-preserving attribute based credentials for 6g networks," in *IEEE Future Networks World Forum (FNWF)*. IEEE, October 2024, pp. 927–932.

[63] L. Bonati, M. Polese, S. D'Oro, S. Basagni, and T. Melodia, "Neutran: An open ran neutral host architecture for zero-touch ran and spectrum sharing," *IEEE Transactions on Mobile Computing*, vol. 23, no. 5, pp. 5786–5798, 2023.

[64] M. Asad, M. Compastié, V. Daza, and M. Siddiqui, "Extending orchestration for privacy preservation in beyond 5g and 6g networks," in *IEEE Future Networks World Forum (FNWF)*. IEEE, October 2024, pp. 372–377.

[65] V. Bolgouras, A. Farao, and C. Xenakis, "Roadmap to secure 6g networks," in *IEEE 29th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, October 2024, pp. 1–6.

[66] S. Drampalou, D. Uzunidis, A. Vetsos, N. Miridakis, and P. Karkazis, "A user-centric perspective of 6g networks: A survey," *IEEE Access*, 2024.

[67] T. Chen, I. Chih-Lin, and T. Melodia, "O-ran's role in shaping 6g: Industry perspectives on open and smart ran," *IEEE Wireless Communications*, vol. 32, no. 1, pp. 10–12, 2025.

[68] D. Vukobratović, N. Bartzoudis, M. Ghassemian, F. Saghezchi, P. Li, A. Aijaz, R. Martinez, X. An, R. Prasad, H. Lüders, and S. Mumtaz, "Distributed sensing, computing, communication, and control fabric: a unified service-level architecture for 6g," *arXiv preprint arXiv:2307.10286*, 2023.

[69] L. Bariah, M. Debbah, H. Sari, and E. Bastug, "Guest editorial: The interplay of digital twin and 6g wireless networks," *IEEE Communications Magazine*, vol. 61, no. 11, pp. 70–71, 2023.

[70] H. Nguyen, K. Sun, D. To, Q. Vien, and T. Le, "Digital twin for o-ran toward 6g," *IEEE Communications Magazine*, 2024.

[71] K. Alam, M. A. Habibi, M. Tammen, D. Krummacker, W. Saad, M. Di Renzo, T. Melodia, X. Costa-Pérez, M. Debbah, A. Dutta, and H. D. Schotten, "A comprehensive tutorial and survey of oran: Exploring slicingaware architecture, deployment options, use cases, and challenges," *IEEE Communications Surveys & Tutorials*, 2025.

[72] V. Zhang, M. Erol-Kantarci, W. Sun, Y. Dai, J. Hoydis, and M. Gursoy, "Guest editorial: Ai and 6g convergence: An energy efficiency perspective," *IEEE Network*, vol. 35, no. 6, pp. 10–11, 2021.

[73] L. Blanco, S. Kukliński, E. Zeydan, F. Rezazadeh, A. Chawla, L. Zanzi, F. Devoti, R. Kolakowski, V. Vlahodimitropoulou, I. Chochliouros, and A. Bosneag, "Ai-driven framework for scalable management of network slices," *IEEE Communications Magazine*, vol. 61, no. 11, pp. 216–222, 2023.

[74] S. Khattak, M. Nasralla, and I. Rehman, "The role of 6g networks in enabling future smart health services and applications," in *IEEE International Smart Cities Conference (ISC2)*. IEEE, September 2022, pp. 1–7.

[75] M. Habibi, B. Han, A. Fellan, W. Jiang, I. Sánchez, A. Pavon, A. Boubendir, and H. Schotten, "Toward an open, intelligent, and end-to-end architectural framework for network slicing in 6g communication systems," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 1615–1658, 2023.

[76] J. Parra-Ullauri, X. Zhou, S. Moazzeni, R. Hussain, X. Vasilakos, Y. Wu, R. Baby, M. Mahmud, G. Incorvaia, D. Hond, and H. Asgari, "Lifecycle management of trustworthy ai models in 6g networks: The reason approach," *IEEE Wireless Communications*, vol. 32, no. 2, pp. 42–51, 2025.

[77] N. Nahar, K. Andersson, O. Schelén, and S. Saguna, "A survey on zero trust architecture: Applications and challenges of 6g networks," *IEEE Access*, 2024.

[78] L. Shen, K. Feng, and L. Hanzo, "Five facets of 6g: Research challenges and opportunities," *ACM Computing Surveys*, vol. 55, no. 11, pp. 1–39, 2023.

[79] L. Yang, S. Naser, A. Shami, S. Muhaidat, L. Ong, and M. Debbah, "Towards zero touch networks: Cross-layer automated security solutions for 6g wireless networks," *IEEE Transactions on Communications*, 2025.

[80] H. Sun, Y. Liu, A. Al-Tahmeesschi, A. Nag, M. Soleimanpour-Moghadam, B. Canberk, H. Arslan, and H. Ahmadi, "Advancing 6g: Survey for explainable ai on communications and network slicing," *IEEE Open Journal of the Communications Society*, 2025.

[81] S. Maxenti, R. Shirkhani, M. Elkael, L. Bonati, S. D'Oro, T. Melodia, and M. Polese, "Autoran: Automated and zero-touch open ran systems," *arXiv preprint arXiv:2504.11233*, 2025.

[82] M. Ameur, B. Brik, and A. Ksentini, "Dual self-attention is what you need for model drift detection in 6g networks," *IEEE Transactions on Machine Learning in Communications and Networking*, 2025.

[83] G. Fontanesi, F. Ortíz, E. Lagunas, L. Garcés-Socarrás, V. Baeza, M. Vázquez, J. Vásquez-Peralvo, J. Minardi, H. Vu, P. Honnaiah, and C. Lacoste, "Artificial intelligence for satellite communication: A survey," *IEEE Communications Surveys & Tutorials*, 2025.

[84] D. Sah, M. Vahabi, and H. Fotouhi, "A comprehensive review on 5g iiot test-beds," *IEEE Transactions on Consumer Electronics*, 2025.

[85] M. Martalò, G. Pettorru, and L. Atzori, "A cross-layer survey on secure and low-latency communications in next-generation iot," *IEEE Transactions on Network and Service Management*, vol. 21, no. 4, pp. 4669–4685, 2024.

[86] B. Brik, H. Chergui, L. Zanzi, F. Devoti, A. Ksentini, M. Siddiqui, X. Costa-Pèrez, and C. Verikoukis, "Explainable ai in 6g o-ran: A tutorial and survey on architecture, use cases, challenges, and future research," *IEEE Communications Surveys & Tutorials*, 2024.

[87] T. Nguyen, H. Nguyen, A. Ijaz, S. Sheikhi, A. V. Vasilakos, and P. Kostakos, "Large language models in 6g security: challenges and opportunities," 2024.

[88] A. Blika, S. Palmos, G. Doukas, V. Lamprou, S. Pelekis, C. Kontoulis, C. Ntanos, and D. Askounis, "Federated learning for enhanced cybersecurity and trustworthiness in 5g and 6g networks: A comprehensive survey," *IEEE Open Journal of the Communications Society*, 2024.

[89] G. Boateng, H. Sami, A. Alagha, H. Elmekki, A. Hammoud, R. Mizouni, A. Mourad, H. Otrok, J. Bentahar, S. Muhaidat, and C. Talhi, "A survey on large language models for communication, network, and service management: Application insights, challenges, and future directions," *IEEE Communications Surveys & Tutorials*, 2025.

[90] S. Shafaei, A. Palaios, Z. Ennaceur, J. Zhang, V. Pandit, P. Gautam, A. Gharouni, B. Gajic, B. Banerjee, S. B. Mallikarjun, M. A. Habibi, M. Danger, C. Wietfeld, and ..., "Towards ai in 6g: Concepts, techniques, and standards," *IEEE Access*, vol. 13, pp. 143 843–143 874, 2025.

[91] V. Charpentier, G. Landi, E. Giannopoulou, J. Brenes, M. Camelo, J. Marquez-Barja, and N. Slamnik-Kriještorac, "Advancing vertical services for 6g: Future directions and innovations," *IEEE Network*, vol. 32, no. 2, pp. 42–51, 2025.

[92] C. González, S. Giménez-Antón, M. Tarzán-Lorente, H. Chergui, and C. Fernández-Martínez, "Extending intent-powered network management with lms in b5g infrastructures," in *IEEE 11th International Conference on Network Softwarization (NetSoft)*. IEEE, June 2025, pp. 1–6.

[93] B. Gort, G. Kibalya, and A. Antonopoulos, "Attention-driven ai model generalization for workload forecasting in the compute continuum," *IEEE Transactions on Machine Learning in Communications and Networking*, 2025.

[94] B.J.Gort, G. Kibalya, and A. Antonopoulos, "Aero: Adaptive edge-cloud orchestration with a sub-1k-parameter forecasting model," *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 3, pp. 463–478, March 2025.

[95] B. Gort, G. Kibalya, M. Serrano, and A. Antonopoulos, "Forecasting trends in cloud-edge computing: Unleashing the power of attention mechanisms," *IEEE Communications Magazine*, 2024.

[96] J. Camargo, E. Coronado, W. Ramirez, D. Camps, S. Deutsch, J. Pérez-Romero, A. Antonopoulos, O. Trullols-Cruces, S. Gonzalez-Diaz, B. Otura, and G. Rigazzi, "Dynamic slicing reconfiguration for virtualized 5g networks using ml forecasting of computing capacity," *Computer Networks*, vol. 236, p. 110001, 2023.

[97] B. Gort, G. M. Kibalya, and A. Antonopoulos, "Agentedge: Agentic ai for service orchestration in the edge-cloud continuum," TechRxiv, 2025, preprint. [Online]. Available: https://www.techrxiv.org/articles/preprint/AgentEdge_Agentic_AI_for_Service_Orchestration_in_the_Edge-Cloud_Continuum/

[98] Y. Xiao, G. Shi, and P. Zhang, "Towards agentic ai networking in 6g: A generative foundation model-as-agent approach," 2025.

[99] A. Salama, Z. Nezami, M. M. Qazzaz, M. Hafeez, and S. A. R. Zaidi, "Edge agentic ai framework for autonomous network optimisation in o-ran," 2025, preprint; arXiv ID not found. Remove this note once a valid eprint is available.

[100] M. Elkael, S. D'Oro, L. Bonati, M. Polese, Y. Lee, K. Furueda, and T. Melodia, "Agentran: An agentic ai architecture for autonomous control of open 6g networks," 2025.

[101] I. Chatzistefanidis, N. Nikaein, A. Leone, A. Maatouk, L. Tassioulas, R. Morabito, I. Pitsiorlas, and M. Kountouris, "Agoran: An agentic open marketplace for 6g ran automation," 2025.

[102] I. Chatzistefanidis, A. Leone, A. Yaghoubian, M. Irazabal, S. Nassim, L. Bariah, M. Debbah, and N. Nikaein, "Mx-ai: Agentic observability and control platform for open and ai-ran," 2025.

[103] X. Li, W. Shi, H. Zhang, C. Peng, S. Wu, and W. Tong, "The agentic-ai core: An ai-empowered, mission-oriented core network for next-generation mobile telecommunications," *Engineering*, 2025.

[104] H. Zhang, Q. Xu, L. Zhao, and S. Li, "Enhancing generative ai reliability via agentic ai in 6g-enabled edge computing," *Communications Engineering*, 2025.

[105] X. Wang, Y. Zhang, J. Lin, and H. Zhao, "A task-driven design approach for 6g ai-native architecture," *Digital Communications and Networks*, 2025.

[106] K. Dev, S. A. Khowaja, E. Zeydan, and M. Debbah, "Advanced architectures integrated with agentic ai for next-generation wireless networks," 2025.

[107] R. Zhang, G. Liu, Y. Liu, C. Zhao, J. Wang, Y. Xu, D. Niyato, J. Kang, Y. Li, S. Mao, S. Sun, X. Shen, and D. Kim, "Toward edge general intelligence with agentic ai and agentification: Concepts, technologies, and future directions," 2025.

[108] M. Zohaib, M. A. Akbar, M. U. Ahmed, H. Malik, H. Al-Kanj, S. Ali, and M. Usman, "Agentic ai in 6g software businesses: A layered maturity model," 2025.

[109] M. M. Saeed, R. A. Saeed, M. K. Hasan, and E. Ali, "A comprehensive survey on 6g-security: physical, connection and service layers," *Discover Internet of Things*, vol. 5, no. 1, pp. 1–25, 2025.

[110] P. K. Gkonis, A. Giannopoulos, N. Nomikos, P. Trakadas, L. Sarakis, and X. Masip-Bruin, "A survey on architectural approaches for 6g networks: Implementation challenges, current trends, and future directions," *Telecom*, vol. 6, no. 2, p. 27, 2025.

[111] M. S. Akbar, H. Malik, F. Hussain, and S. Ali, "On challenges of sixth-generation (6g) wireless networks: A survey," *Journal of Network and Computer Applications*, vol. 236, p. 103896, 2025.

[112] N. F. S. de Sousa, S. Clayman, F. Slyne, and L. Mamatas, "Network service orchestration: A survey," *Computer Communications*, vol. 140, pp. 62–94, 2019.

[113] Z. Xiao, C. Ye, Y. Hu, H. Yuan, Y. Huang, L. Cai, J. Chang, and Y. Feng, "Llm agents as 6g orchestrator: A paradigm for task-oriented physical-layer automation," in *2024 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2024, pp. 1–6.

[114] I. Ullah, A. Arishi, S. K. Singh, F. Alharbi, A. H. Ibrahim, M. Islam, Y. I. Daradkeh, and C. Choi, "Autonomous network management for 6g communication: A comprehensive survey," *Digital Communications and Networks*, 2025.

[115] A. Mekrache, A. Ksentini, and C. Verikoukis, "Next-generation 6g network management with oss-gpt," in *Proceedings of the ACM SIGCOMM 2025 Posters and Demos*. ACM, 2025, pp. 158–160.

[116] E. Evgenieva, A. Vlahov, A. Ivanov, V. Poulkov, and A. Manolova, "A comprehensive survey of 6g simulators: Comparison, integration, and future directions," *Electronics*, vol. 14, no. 16, p. 3313, 2025.

[117] A. Omar, X. Li, and R. Chen, "Intelligent control in 6g open ran: Security risk or opportunity?" 2025, preprint; arXiv ID not found. Remove this note once a valid eprint is available.

[118] J. Smith, M. Wang, C. Hernandez, and A. Gupta, "Security testing the o-ran near-rt ric & a1 interface: Lessons from onos and osc," in *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, 2025, pp. 3456–3469.

[119] W. Zhang, T. Ahmed, and M. Bianchi, "Towards secure intelligent o-ran architecture: A layered threat model and defense perspective," *IEEE Communications Standards Magazine*, vol. 9, no. 2, pp. 45–53, 2025.

[120] M. Yang, Y. Qu, T. Ranbaduge, C. Thapa, N. Sultan, M. Ding, H. Suzuki, W. Ni, S. Abuadbba, D. Smith, and P. Tyler, "From 5G to 6G: A survey on security, privacy, and standardization pathways," 2024. [Online]. Available: https://arxiv.org/abs/2410.21986

[121] H. Lee, R. Kumar, and X. Chen, "Privacy-preserving ai framework for 6g-enabled consumer electronics," *ACM Transactions on Internet Technology*, vol. 25, no. 3, pp. 1–23, 2025.

[122] B. Brik, H. Chergui, L. Zanzi, F. Devoti, A. Ksentini, M. S. Siddiqui, X. Costa-Pèrez, and C. Verikoukis, "Explainable ai in 6g o-ran: A tutorial and survey on architecture, use cases, challenges, and future research," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 2, pp. 1321–1358, 2024.

[123] H. X. Nguyen, K. Sun, D. To, Q. T. Vien, and T. A. Le, "Digital twin for o-ran toward 6g," *IEEE Communications Magazine*, vol. 63, no. 3, pp. 174–181, 2024.

[124] S. Niknam, A. Roy, H. S. Dhillon, S. Singh, R. Banerji, J. H. Reed, N. Saxena, and S. Yoon, "Intelligent O-RAN for beyond 5g and 6g wireless networks," in *2022 IEEE Globecom Workshops (GC Wkshps)*. Rio de Janeiro, Brazil: IEEE, Dec. 2022, pp. 215–220.

[125] S. Gopal, A. Kord, and R. A. Rouil, "O-ran and 6g: The future of wireless innovation?" *arXiv preprint arXiv:2411.09959*, 2024.

[126] S. Singh and U. Samal, "Insights and trends in open ran: The future of mobile networks," *Journal of Network and Systems Management*, vol. 33, no. 2, pp. 1–34, 2025.

[127] M. Polese, M. Dohler, F. Dressler, M. Erol-Kantarci, R. Jana, R. Knopp, and T. Melodia, "Guest editorial open ran: A new paradigm for open, virtualized, programmable, and intelligent cellular networks," *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 2, pp. 241–244, 2024.

[128] V. Kasuluru, L. Blanco, E. Zeydan, A. Bel, and A. Antonopoulos, "Enhancing cloud-native resource allocation with probabilistic forecasting techniques in o-ran," in *2024 Joint European Conference on*

Networks and Communications & 6G Summit (EuCNC/6G Summit). IEEE, June 2024, pp. 1–6.

Saher Pervaiz is pursuing MS in Computer Science at The University of Chenab, Gujrat, Pakistan. Her research interests include Zero-touch Network and Service Management (ZSM), explainable AI, federated learning, NLP, and 6G automation.

Sonia Shahzadi is currently serving as an Assistant Professor at the Air University, Pakistan. Her research interests are centered on advancing next-generation network architectures, leveraging key enablers of B5G/6G networks such as intent-based orchestration, zero-touch network and service management (ZSM), network function virtualization (NFV), and distributed edge paradigms, including cloudlets and fog computing.

Anwer Al-Dulaimi (Senior Member, IEEE) received the Ph.D. degree in Electrical and Computer Engineering from Brunel University London, U.K., in 2012. He is currently with the CTO Office, Veltris, Toronto, Canada. Previously, he was a Senior Research Scientist at EXFO and the Technical Lead of 5G/6G innovation projects at the National Research Council of Canada. He has served as the Editor and Guest Editor for several IEEE journals and has contributed to standardization activities with IEEE and ITU-T. His research interests include wireless network architecture, edge and cloud computing, AI-enabled communications, and 6G system design.

Dr. Al-Dulaimi is a Senior Member of the IEEE and has authored or coauthored more than 100 journal and conference papers and several book chapters. He also coedited the book *6G Enabling Technologies: Beyond 5G Mobile Networks* (Wiley, 2020).

Chih-Lin I (Fellow, IEEE) received the Ph.D. degree in electrical engineering from Stanford University, Stanford, CA, USA. She is currently the Chief Scientist of Wireless Technologies with the China Mobile Research Institute (CMRI), Beijing, China. Before joining CMRI, she worked at AT&T Bell Laboratories as a Principal Technical Staff Member, served as Director of AT&T Headquarters and ITRI Taiwan, and was Vice President and Group Director at ASTRI Hong Kong.

She leads research and development on green and AI-native wireless networks and established the Green Communications Research Center at CMRI, where she launched the 5G Key Technologies Research and Development program. She is the Chair of the O-RAN Technical Steering Committee and an Executive Committee Member, Chair of the FuTURE 5G/6G SIG, and Chair of the WAIA Executive Committee. Her current research focuses on ICDT Deep Convergence—"From Green and Soft to Open and Smart."