A Survey on Zero Touch Network and Service (ZSM) Management for 5G and Beyond Networks

Madhusanka Liyanage[a], Quoc-Viet Pham[b], Kapal Dev[c], Sweta Bhattacharya[d], Praveen Kumar Reddy Maddikunta[d], Thippa Reddy Gadekallu[d], Gokul Yenduri[d]

[a]*School of Computer Science, University Collage Dublin, Ireland and Centre for Wireless Communications, University of Oulu, Finland*
[b]*Korean Southeast Center for the 4th Industrial Revolution Leader Education, Pusan National University, Busan, Korea*
[c]*Department of institute of intelligent systems, University of Johannesburg, South Africa.*
[d]*School of Information Technology, Vellore Institute of Technology, Vellore, India*

Abstract

Faced with the rapid increase in smart Internet-of-Things (IoT) devices and the high demand for new business-oriented services in the fifth-generation (5G) and beyond network, the management of mobile networks is getting complex. Thus, traditional Network Management and Orchestration (MANO) approaches cannot keep up with rapidly evolving application requirements. This challenge has motivated the adoption of the Zero-touch network and Service Management (ZSM) concept to adapt the automation into network services management. By automating network and service management, ZSM offers efficiency to control network resources and enhance network performance visibility. The ultimate target of the ZSM concept is to enable an autonomous network system capable of self-configuration, self-monitoring, self-healing, and self-optimization based on service-level policies and rules without human intervention. Thus, the paper focuses on conducting a comprehensive survey of E2E ZSM architecture and solutions for 5G and beyond networks. The article begins by presenting the fundamental ZSM architecture and its essential components and interfaces. Then, a comprehensive review of the state-of-the-art for key technical areas, i.e., ZSM automation, cross-domain E2E service lifecycle management, and security aspects, are presented. Furthermore, the paper contains a summary of recent standardization efforts and research projects toward the ZSM realization in 5G and beyond networks. Finally, several lessons learned from the literature and open research problems related to ZSM realization are also discussed in this paper.

Keywords: Zero-touch network and Service Management, Machine Learning, Artificial Intelligence, Security, 5G, 6G, Service Management, Automation, Orchestration

1. Introduction

Owing to the emergence of new applications such as autonomous vehicles and virtual reality, as well as the proliferation of massive Internet-of-Things (IoT) services, numerous technologies have been developed for fifth-generation (5G) and beyond 5G (B5G) networks. Among the potential technologies, network function virtualization (NFV), software-defined networking (SDN), network slicing (NS), and multi-access edge computing (MEC) have been considered as crucial enablers of 5G, and B5G networks [1, 2, 3, 4]. In NFV, the network functions are decoupled from the underlying hardware which enables fast deployment of new services and also enables quick adaptability to scalable yet agile needs of the customers [5]. Furthermore, SDN allows network configuration and monitoring in a dynamic and programmed manner, helping

Email addresses: madhusanka@ucd.ie, madhusanka.liyanage@oulu.fi (Madhusanka Liyanage), vietpq@pusan.ac.kr (Quoc-Viet Pham), kapal.dev@ieee.org (Kapal Dev), sweta.b@vit.ac.in (Sweta Bhattacharya), praveenkumarreddy@vit.ac.in (Praveen Kumar Reddy Maddikunta), thippareddy.g@vit.ac.in (Thippa Reddy Gadekallu), gokul.yenduri@vit.ac.in (Gokul Yenduri)

to manage the entire network holistically and globally regardless of the underlying technologies [6]. MEC is another key technology that moves computing resources and IT functionalities from the central cloud to the network edge close to IoT and mobile users [2]. NS, on the other hand, is a critical technology that facilitates service customization and resource isolation, enabling multiple logical networks on the same physical infrastructure [7]. There exists three primary services that are supported in 5G networks which includes enhanced mobile broadband (eMBB), massive machine-type communication (mMTC), ULTRA-Reliable and Low-Latency Communication (URLLC). It is expected that these services would be supported to a great extent to help unforeseeable applications such as extended reality (XR), holographic Telepresence, and collaborative robots which would be available in 2030. These applications demand joint optimization of computation communication, caching, control and sensing [4].

Network infrastructures and supporting technologies have witnessed immense growth both horizontally and also vertically [8, 9]. The conventional 5G cellular networks are composed of terrestrial infrastructures such as IoT and mobile devices, small cells, and macro-cells. In order to support such massive connectivity ensuring global coverage, future sixth-generation (6G) wireless systems would comprise of underground, underwater, and aerial communications [8]. In particular, an aerial radio access network consists of three main tiers, including low-altitude platforms (LAPs), high-altitude platforms (HAPs), and low-earth orbit (LEO) satellites [9]. LAP systems usually connect to users directly and support very high-quality of services (QoS). The LEO satellite tier supports sparse-connectivity scenarios and global coverage with reasonable QoS, while HAP systems maintain a balance of LAP systems and LEO satellite communications. Along with a massive number of IoT and mobile devices, managing the network in a fully automated manner is a great challenge [4]. Although many solutions and concepts have been developed over the last decade, such as NFV, SDN, MEC, and NS, still manual processes are required for the operation and management of present network systems, i.e., human intervention is a must to ensure fully autonomous network and service management solutions [10, 11, 12]. These difficulties have motivated extra efforts from academic and industry communities.

1.1. Need of Zero-Touch Network and Service Management

The following limitations of existing network management and orchestration (MANO) solutions have motivated the adoption of the Zero-touch network and Service Management (ZSM) concept [13, 14, 15, 16, 17, 18, 19, 20, 21, 22].

- **Network Complexity**: Massive IoT connectivity, many emerging services, and new 5G/6G technologies result in extremely heterogeneous and complex mobile networks, and thus significantly increase the overall complexity of the network orchestration and management.
- **New Business-Oriented Services**: Many new services will be available in future networks, which should be quickly implemented to meet business opportunities. Along with key-enabling technologies such as NS, NFV, and MEC, the ZSM concept allows an agile and more straightforward deployment of new services.
- **Performance Improvement**: Diverse QoS requirements and the need to reduce the operational cost and improve network performance triggers robust solutions of network operation and service management.
- **Revolution for Future Networks**: Even 5G networks are not fully available worldwide, numerous activities have been dedicated to the research and development of future 6G wireless systems. Many new technologies, services, applications, and IoT connections will be available, which will make the future network very complex and complicated to be efficiently managed by conventional MANO approaches [4].

The above limitations explain a strong need for the ZSM concept for the complete automation and management of future networks. In order to eliminate such limitations, enabling fully automated network operation and management solutions, the European Telecommunications Standards Institute (ETSI) ZSM group was established in December 2017.

1.2. Importance of ZSM for 5G and Beyond

The recent advancements in IoT technology increase the number of connected devices [23]. As the number of devices increases, there is a need to improve network infrastructure to ensure good communication or connectivity among geographically spread devices [24]. These advancements should enable real-time operations to be performed with minimal latency and improved performance. To be successful in achieving these goals, a suitable communication medium is required. 5G and beyond is the promising next-generation network that enables various enhanced capabilities such as ultra-low latency, high reliability, seamless connection, and mobility support [25]. To meet enterprise requirements, 5G is built with service-aware globally managed infrastructures, highly programmable. SDN, NFV, MEC, and NS are critical foundations for 5G and beyond [26]. New business models such as multi-domain, multi-service, and multi-tenancy, will emerge in 5G and beyond due to new technologies, thus bolstering new industry dynamics. The existing infrastructure will result in a complex 5G architecture in terms of operations and services [27].

Traditional network management techniques do not fulfill the new paradigm, hence the need arises for an efficient end-to-end (E2E) automated network system capable of providing faster services to end-users [28]. The goal of automation is to drive services through an autonomous network governed by a set of high-level policies and rules. Enabled by the ZSM implementation, 5G and beyond networks can be operated independently, i.e., without human intervention [29]. Keeping the requirements in the account, ETSI developed the ZSM ISG in 2017. The ZSM objective is to create an underlying paradigm that enables fully autonomous solutions for network operation and service management of 5G and beyond networks. The ZSM comprises operational processes and tasks such as planning, delivery, deployment, provisioning, monitoring, and optimization that are executed automatically without human intervention [30].

1.3. Paper Motivation and Paper Contributions

There have been researching works on the adoption of B5G technologies for ZSM systems. For example, Bunyakitanon *et al.* [11] investigated a deep reinforcement learning (DRL) approach, namely AREL3P, to enhance the performance of the autonomous placement of VNFs. Some results using a real 5G testbed show an improved accuracy of 45% of the AREL3P approach and significant outperformance compared with benchmarks using supervised learning techniques. Recently, Moazzeni *et al.* [31] proposed a novel profiling method to enable autonomous NFV orchestration in next-generation network. In particular, the proposed profiling framework is composed of three main blocks, including the resource configuration selector, the analyzer and processor, and the predictor. The experimental results show that the learning model from the third block can achieve very close performance compared with the actual one. These works have shown the need for ZSM to significantly reduce the operational cost and increase next-generation networks' operation.

Owing to the paramount importance of ZSM for fully autonomous operation and management of 5G and B5G networks, some research works have been carried out to summarize the topic. Considered as key enablers of ZSM, comprehensive surveys on MEC, NS, SDN, NFV, and MEC were presented in [2], [7], [32], and [33], respectively. However, these surveys only focus on a specific topic, such as edge computing and network virtualization, while a comprehensive survey on ZSM for 5G and beyond networks has not been carried out. Benzaid and Taleb [10] discussed that despite a key enabler of ZSM in B5G networks, there are inherent limitations and significant challenges of using artificial intelligence (AI) and big data analytics. Lack of labeled datasets, AI model explainability, model accuracy, computation complexity, and new security threats are examples of AI-driven ZSM approaches. In the light of discussions on these limitations, potential solutions are emphasized in [10], including collaborative learning, AI trust, design of low-complexity AI models, the tradeoff of training overhead, and AI model performance, and adversarial AI. Recently, Gallego-Madrid *et al.* [34] reviewed the applications of machine learning (ML) for ZSM and discussed some potential directions, such as lack of data, cross-layer intelligence, security, computational complexity, and scalability. Furthermore, in [35], security threats of ZSM automated systems are reviewed, and several potential solutions are proposed. Addressing these security threats is of paramount importance as ZSM systems are built from many technologies. Each one causes distinct security challenges. For example, virtual network functions (VNFs) are vulnerably affected by software designs and undesirable configurations. Thus the incorrect data provided by VNFs would lead to inappropriate service and management of the ZSM

Table 1: Summary of related review papers on ZSM for 5G and beyond networks.

Reference	Contributions	Limitations
[2], [7], [32], [33]	These papers provide comprehensive surveys on key enablers of ZSM, including MEC in 5G and beyond [2], NS and softwarization [7], SDN [32], and NFV [33].	These works only focus individual key technologies (e.g., MEC, NS, SDN, and NFV), i.e., they do not focus on ZSM.
[10]	This magazine provides high-level discussions on the challenges and limitations of AI and big data when they are applied to solve ZSM problems.	Only the limitations and risks of AI-based approaches are presented for the ZSM realization.
[34]	This survey provides an overview of ZSM and the applications of ML for ZSM management and orchestration.	Some important aspects of ZSM are not presented, such as E2D service lifecycle management and standardization.
[35]	This magazine focuses on security challenges in ZSM and highlights a number of potential solutions.	This work only discusses security aspects of ZSM, while important aspects of ZSM are not presented.
[36]	This magazine illustrates the application of AI for NS resource allocation problems.	This work primarily focuses on the use of AI for resource allocation in NS, while ZSM is ignored.
This work	A comprehensive survey on the ZSM concept in 5G and beyond networks, from ZSM fundamentals and ZSM automation to ZSM security and ZSM standardizations and projects. Moreover, we present important lessons learnt from the open literature and discuss potential research directions to realize ZSM in 5G and beyond networks.	

framework. Recently, Bega *et al.* [36] reviewed the applications of AI for functions and resources allocations in zero-touch NS systems, from admission control to resource orchestration and slice scheduling. However, several aspects of ZSM have not been presented in [10, 35, 36], such as applications of ZSM in 5G and standardization efforts and real projects toward the realization of ZSM in 5G and beyond. The summary of these related papers and our work is presented in Table 1.

Although ZSM has been studied in the literature, no existing studies have been dedicated to providing a comprehensive survey on ZSM in 5G and beyond networks. This limitation motivates to conduct a more comprehensive survey on the ZSM architecture and solutions for 5G and beyond networks. The contributions of this work lie in an extensive discussion of ZSM fundamentals, architecture requirements, components, interfaces, and automation. Furthermore, research activities standardization efforts toward the ZSM realization are also presented. Finally, the key lessons learnt from the reviewed literature and a number of promising research directions are also presented. In sum, the contributions and features offered by our survey can be summarized as follows.

- **Provide an overview of ZSM**: This paper first presents the fundamentals of ZSM, including the ZSM reference architecture, architecture design principles, architecture requirements, and security requirements.
- **Discuss ZSM automation**: As the goal of ZSM is to ensure all the networks to be executed and managed automatically, automation may have different means and aspects. In this regard, we overview different means of automation, including policy-driven automation, intent-based networking, intent-based service orchestration, network governance, network stability, and use of AI techniques such as transfer learning and deep reinforcement learning.
- **Present cross-domain E2E service lifecycle management**: We summarize management processes towards the cross-domain E2E service lifecycle such as on-boarding process, fulfillment process, assurance process, and optimization.

- **Review security aspects of ZSM**: Potential security of ZSM systems are summarized. In particular, we discuss security issues in E2E service management service, data collection, service analytics, service intelligence, service orchestration, policy management, and closed-loop automation.
- **Summarize standardization efforts and projects**: Popular projects towards the development and implementation of ZSM in B5G networks are summarized. The standardization efforts and activities are also summarized in this paper
- **Highlight the challenges and future research directions**: Various challenges in making full automation of B5G and future 6G wireless systems are spotlighted along with potential research directions.

Table 2: Summary of Important Acronyms.

Acronym	**Definition**	**Acronym**	**Definition**
5G	Fifth-Generation	6G	Sixth-Generation
A2A	Automatic to Autonomous	AI	Artificial Intelligence
B5G	Beyond 5G	CSI	Channel State Information
DASA	Dynamic Auto-Scaling Algorithm	DL	Deep Learning
DoS	Denial of Service	DDoS	Distributed DoS
DRL	Deep Reinforcement Learning	E2E	End-to-End
eMBB	enhanced Mobile Broadband	ETSI	European Telecommunications Standards Institute
HAP	High-Altitude Platform	IBN	Intent-Based Networking
ICT	Information and Communication Technology	IDM	Intent-Driven Management
IGA	Iterative Gradient Attack	IoT	Internet-of-Things
IP	Internet Protocol	ISG	Industry Specification Group
LAP	Low-Altitude Platform	LC	Life-cycle
LEO	Low-Earth Orbit	MANO	Management and Orchestration
MD	Management Domain	MEC	Multi-access Edge Computing
MEC	Multi-access Edge Computing	MITM	Man-In-The-Middle
ML	Machine Learning	MMG	Monitoring Model Generator
MMG	Monitoring Model Generator	mMTC	massive Machine-Type Communication
NFV	Network Function Virtualization	NS	Network Slicing
QoS	Quality of Service	SDN	Software-Defined Networking
SDO	Standards Development Organisation	URLLC	Ultra-Reliable Low-Latency Communication
VNF	Virtualized Network Function	XR	eXtended Reality
ZSM	Zero Touch Network and Service Management	ZTM	Zero Touch Management

1.4. Outline of The Paper

The organization of this paper is as follows. In Section 2, the fundamental architecture of ZSM in the 5G context is provided, where key components and interfaces are presented. Section 3 reviews the state-of-the-art studies on ZSM automation, which is followed by the cross-domain services in Section 4. In Section 5, we comprehensively review different security aspects of ZSM in detail. Next, recent standardization efforts and projects toward the ZSM realization in 5G and beyond networks are summarized in Section 6. Several lessons learned from the literature and potential research directions are highlighted in Section 7. Finally, the paper is concluded in Section 8. For ease of following, a list of important acronyms are presented in Table 2.

2. Overview of Zero Touch Network and Service Management

One of the main design objectives of the ZSM reference architecture is its ability to achieve zero-touch enabled network and service management, irrespective of the vendors. The ZSM reference architecture provides flexible management services, which aligns with the industry trend of alienating from the management systems [10]. A detailed discussion on the ZSM reference architecture, its key components, and interfaces is provided in this section.

2.1. ZSM Architecture Principles

ZSM is designed based on the principle of supporting self-contained, loosely-coupled facilities. It allows the accommodation of new services and the modules to be scaled and deployed independently. ZSM architecture facilitates portability, re-usability, vendor-neutral resource and service management. The use of closed-loop management automation is to achieve and maintain a set of goals without any intervention. It allows management functions to be separated from the data storage and processing [37].

Management services are planned in such a way that they can resume their regular services after the issues have been resolved. Services are managed based on these resources in a management domain. Exterior to the management domain, the domain resource's complexity can be abstracted from the service users. The E2E cross-domain service management coordinates the management domain activities and manages E2E services that span across management domains. The management domains expose the management resources. These management resources can be merged to form new management services. The intent-based interfaces are exposed to high-level abstractions, and the behavior of related entities are interpreted [38].

The architecture is simple and satisfies all the functional and non-functional specifications. The components and functionalities of the ZSM architecture assist in network and service management's automation.

2.2. ZSM Architecture Requirements

The ZSM reference architecture specifications are derived from ETSI GS ZSM 001 scenarios and requirements [10]. It also identifies functional and nonfunctional requirements that have to be satisfied by the architecture [39, 40, 41, 42].

2.2.1. Non-functional Requirements

General non-functional requirements. The ZSM reference architecture is expected to support the ability to achieve a defined degree of availability, wherein the management actions would be able to comply with relevant regulatory requirements accordingly. Furthermore, it should be energy efficient and remain independent from the vendor, the operator, and the service provider.

Non-functional requirements for cross-domain data services. The ZSM platform reference architecture is expected to accommodate QoS specifications for data services in and outside the ZSM framework reference architecture. It should achieve high data availability and capabilities to process the data. It should also possess the ability to complete management tasks in a predetermined amount of time.

Non-functional requirements for cross-domain service integration. The ZSM reference architecture provides new and legacy management functions. The changes in the management functions should not be required to integrate management resources into the ZSM framework. ZSM framework reference architecture is expected to allow management resources to be added or removed on demand and also enable multiple management service versions to coexist at the same time.

2.2.2. Functional requirements

General functional requirements. The ZSM framework reference architecture should provide frameworks for managing the services and the resources, including resource facing service and customer facing service that are provided by the management domains. In addition, adaptive closed-loop management and cross-domain management of E2E resources should be supported. It needs to enable the operator to have a constrained automated decision-making processes with rules and policies. Any ambiguity of management domains and E2E services is to be hidden. All the technology domains required to implement an E2E service should be supported.

Automation of operational life cycle management functions should be promoted by the ZSM management domains that apply to the services and the resources. The ZSM framework reference architecture should provide access control and open interfaces.

Functional requirements for data collection. The ZSM architecture needs to provide functionality that allows collecting live data, providing features for storing the collected data. The live data collected should be allowed to be accessed such that relevant data governance techniques can be implemented ensuring shared access is provided for inter-domain aggregation and (pre-)processing/filtering is performed on the collected data. The reference architecture of the ZSM should allow various kinds and levels of data with cadence, velocity and volume. The distribution of the collected data should be done as per the needs, keeping it consistent, allowing metadata to be attached to the same [42].

Functional requirements for cross-domain data services. The reference architecture of the ZSM needs to support data services across the domains to provide features that allow data storage to be separated from the data processing, where data has to be shared within the reference architecture. It is expected to offer features that will enable automatic data recovery, redundancy management in stored data, consistency, data service failure, and overload handling. It should also provide capabilities for logically centralized data storage processing based on the policies of multiple data resources with various data types [43].

Functional requirements for cross-domain service integration and access. The ZSM framework reference architecture should provide functionality that allows management resources to be registered, discovered thereby offer details regarding access to the discovered services. Furthermore, it should enable asynchronous and synchronous communication between consumers and service producers. It should provide features that make it easier to invoke management resources indirectly ensuring that the direct invocation of the discovered management resources by the service user are not prohibited by ZSM [44].

Functional requirements for lawful intercept. The undetectable attribute of lawful intercept should be assisted by the ZSM architecture endorsing the ability to prevent lawful interception from being interrupted [45].

2.2.3. Security Requirements

The ZSM framework reference architecture must include features that allow data protection in use, in transit and at rest. An optimum level of security is expected in the management functions, managed services, and infrastructure resources. It should ensure security of management data, integrity of data, management of services, infrastructure resources and functions. Furthermore, it needs to ensure the availability of infrastructure resources, data, management functions. The managed services should include personal data privacy features like privacy-by-design and privacy-by-default. Authenticated service users should approve service access using the ZSM framework reference architecture endorsing the ability to automatically implement acceptable security policies based on the individual management services and its compliance status concerning security requirements. Automated attack/incident detection, recognition, prevention and mitigation should also be supported. To avoid the spread of vulnerabilities and attacks, the ZSM platform reference architecture should enable capabilities to supervise/audit the decisions of the ML/AI on privacy and security issues [46].

2.3. Reference Architecture

The architecture of the ZSM was created to fully automate the network and service management in the environments with multi-domains, where the operations span across the legal boundaries of the organizations [47, 48]. Cross-domain data services, multiple management domains (MDs), intra- and cross-domain integration fabrics, and an E2E service MD are all part of the system architecture, as shown in Fig. 1.

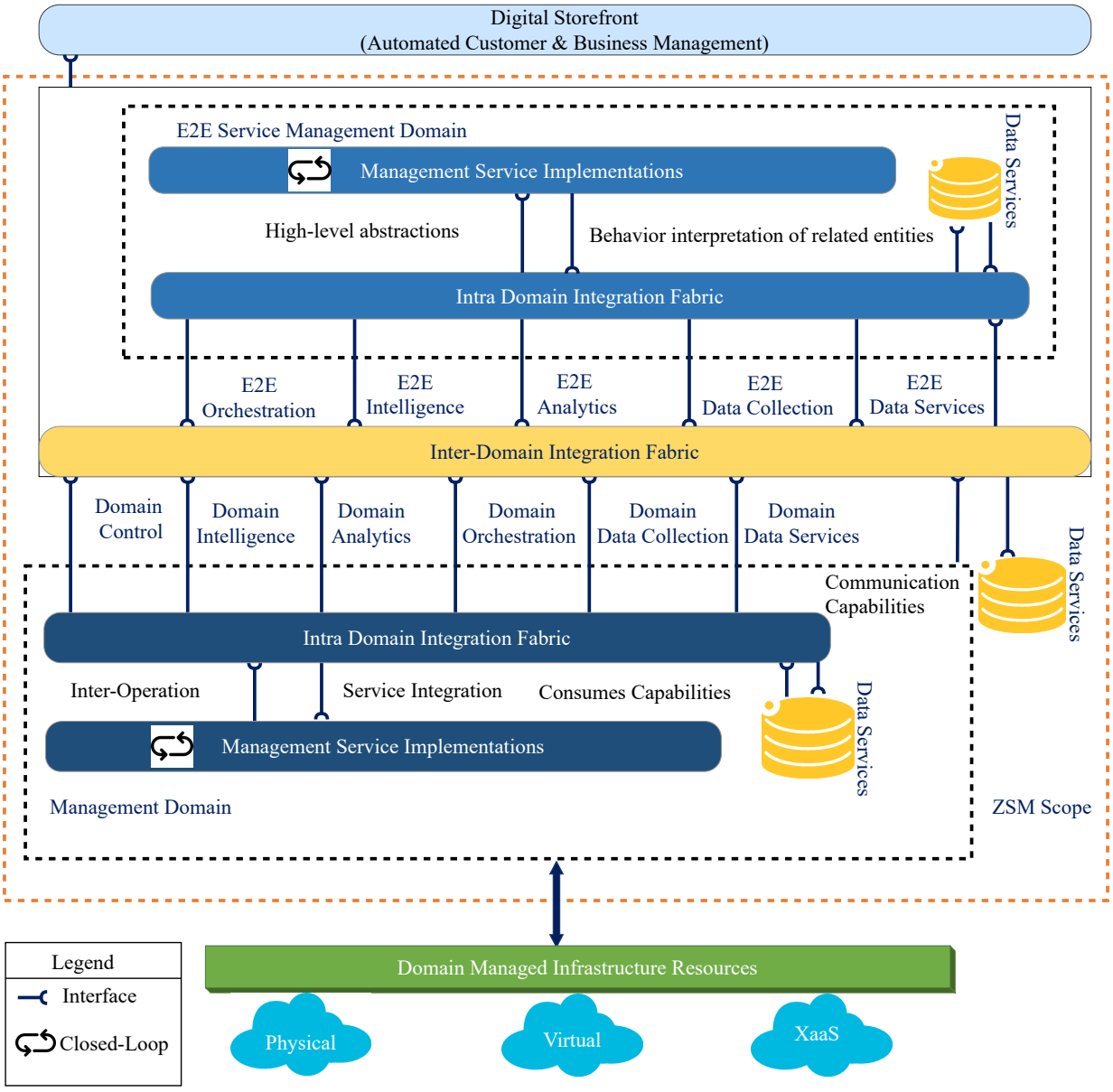

Figure 1: The ZSM framework reference architecture [14].

Every MD is responsible for smart automated resource and service management within their scope. The E2E service MD is treated as an in-charge of E2E service management across various administrative domains. The differentiation of MDs and E2E service MDs encourages device modularity and helps them to grow independently. Each MD is made up of several management functions organized into logical groups through which service interfaces are exposed by management services [49].

The intra-domain integration fabric is used to provide and consume resources that are local to the MD. The cross-domain integration fabric consumes resources that are spread across domains. Intelligence services within E2E service MDs and MDs may use data in cross-domain data services to support cross-domain, and domain-level AI-based closed-loop automation [50].

2.4. Components

The components of the ZSM reference architecture are discussed in brief below.

Management services. The fundamental building block in the ZSM architecture is its "management service." Management services provide capabilities for consumption by consumers with the help of standardized management service end-points. A management service's capabilities collectively describe its role in the organization it manages. Multiple service customers may use the same service capabilities. Several service end-points may be allocated to one or more service capabilities. For invocation, all management services have a consistent collection of capabilities. In the case of interactions between management domains, it allows a high degree of automation and consistency. Management services that are already available can be merged to create new management services. Management resources with higher abstraction and broader reach are supported by each higher layer in the composition hierarchy. The infrastructure resources communicate with the management service producers to provide their capabilities, either directly through their management interfaces or indirectly through the consumption of other management services through their service end-points [51].

Management functions. Management functions produce and use management services, which can be both producer and consumer of the service. If the management function produces certain capabilities, it is a service producer. On the contrary, it is a service consumer if it consumes certain management services [52].

Management domains. The administrative responsibilities are classified by the management domains to establish "separation of concerns" in a given ZSM framework, depending on several implementation, organizational, governance, and functional constraints. It federates management services with the capabilities required to control the resources/resource-facing services in a given domain. For example, some management services are constrained by approvals when the authorized consumers consume the management domain. In contrast, others remain available to the authorized consumers, both within and outside the management domain, at all times. Management domains manage one or more entities and provide service capabilities by consuming service end-points. Sometimes, the consuming service being managed by the management domain can also potentially consume management services [53].

The E2E service management domain. It is a unique management domain that offers E2E management of customer-facing services, combining resource-facing services from several management domains. However, it does not control infrastructure resources directly [54].

Integration fabric. It facilitates communication and inter-operation between management functions that include the communication between management functions, discovery, registration, and invocation of management services. It also offers management service integration, inter-operation, communication capabilities, and consumes capabilities [55].

Data services . Registered consumers can access and persist shared management data across management services using the data services. Data processing and data persistence are enabled by removing management functions to handle their data persistence [56].

2.5. ZSM Interfaces

Domain data collection. Domain data collection systems track managed services and managed entities, providing fault data and live output to support closed-loop automation, which requires the ability to check how the network responds to changes. Domain intelligence services interact with the domain data collection services, domain control services, domain analytics, and domain orchestration services [57].

Domain Analytics. Domain analytics services produce domain-specific recommendations based on the data obtained by several sources, including domain data collection services [58].

Domain Intelligence. These are responsible for driving a domain's intelligent closed-loop automation by supporting automated decision-making and variable levels of human oversight with the help of autonomous management [59]. The following are the different types of intelligence services: 1) Decision assistance. 2) Decisions making. 3) Assistance in the plan of action.

Domain Orchestration. Domain orchestration is a collection of management services that enable automate workflows and processes within a management domain to control the life-cycle management of managed customer and resource-facing services. It also monitors the network services, and virtual resources handled by the management domain, further governed by policies and several other sources of information [60].

Domain Control. Each entity is controlled individually by the domain controller. The services are provided in the domain orchestration group by the management functions to change the configuration or the state of a consumed service and the controlled entity. The domain control category also provides services for managing virtualized resources [46].

E2E Data Collection. The availability and quality of customer-facing services are tracked by the E2E service data collection services that help monitor the quality of the actual E2E service and check the experience of the end-user based on updated data. The management domains' data collection services provide these data that control the services constituting the E2E service [61].

E2E Analytics. The E2E analytics services provide the root cause analysis and E2E service impact and the generation of service-specific predictions. In addition, E2E service analytics includes testing Service Level Specifications and monitoring Key Performance Indicators [62].

E2E Intelligence. The E2E intelligence services provide intelligent closed-loop automation in the E2E service management domain that allows human oversight and variable levels of automated decision-making [63]. The following are the different types of intelligence services: 1) Decision-making assistance. 2) Making the decisions. 3) Action planning.

E2E Orchestration. These are responsible for catalog-driven E2E orchestration of several management domains to modify/create/delete the customer-facing services across the domains. A service model shows how the different service components are connected and how they are related to the management domains [10].

3. The Pathway - From Automatic to Autonomous (A2A)

Automation refers to the execution of tasks autonomously without the intervention of human actions. Automation can be applied to a wide variety of applications such as business processes, network management, resource allocation, routing protocols, resource optimization, and various others[64]. It is possible to achieve automation through service-based architectures, artificial intelligence (AI)-driven techniques, programmable networks, and soft computing strategies. The main objective behind applying automation is to attain scalability, flexibility, and agility for the aforementioned services, thereby achieving state-of-the-art solutions to numerous predominant problems. ZSM provides the liberty to the vendors and users to get involved in the automation ecosystem through different automation approaches shown in Fig. 2 [64]. According to ETSI, ZSM architecture is designed to provide the necessary speed and agility for digital services concerning network automation. Furthermore, the architecture is expected to be adaptive in nature so the automated features meet the compliance standards for the emerging technologies.

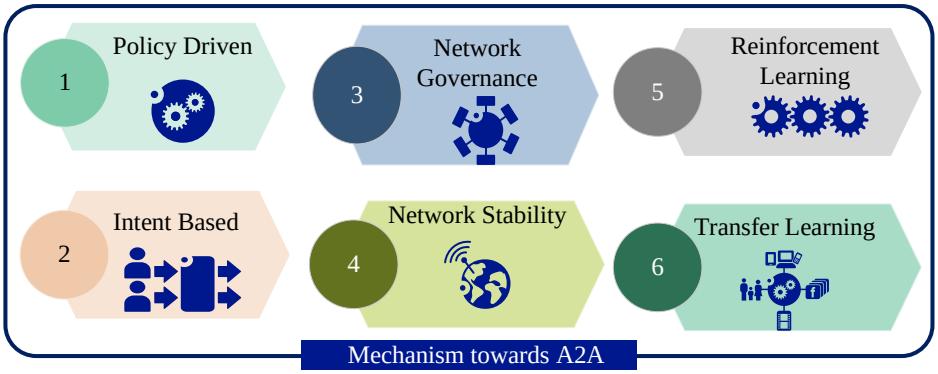

Figure 2: Mechanisms towards A2A.

3.1. Mechanisms for A2A

Various approaches are used to achieve automation and primary intention of all these approaches is to enable a specific or wide variety of functionalities, processes, and tasks concerning agility in network and operational services, respectively. The aim is to achieve the highest abstraction of automation, thereby developing autonomous systems having capability to think and act independently through the combination of adaptive, aware and automatic characteristics or features.

3.1.1. Policy Driven Automation

The existing policy refers to a set of rules that guide the various performance of tasks in an automated manner. As an example, the recent deployments in the networking field use dynamic policies to map changes in network configurations and life-cycle management [65] [66] [67]. In simplistic terms, the policies act as a set of trigger points which, when complied upon, execute the automation measures for specific tasks.

3.1.2. Intent Based

At the initial phases, the intent was used as a synonym for policy-based management. However, lately the word intent has been redefined considering the context of goals and behavioral changes that govern the autonomous characteristics of the management system. Although there is no standard or universally agreed-upon definition for an intent-based system, it is defined as the policy or set of rules wherein the behavioral choices and user-specific goals are used to achieve specific tasks for autonomous services [**?**] [68].

3.1.3. Network Governance

Most of the existing tasks are performed by management systems governed by humans. On the contrary, network governance considers the control of such said tasks by the network itself in an autonomous manner [69] [70]. The network governance can be achieved by defining mechanisms, functionalities, and concepts which includes the means of automation in order to manage network resources and infrastructure, accordingly [71, 72] [73] [74].

3.1.4. Network Stability

In the realm of the aforementioned automation aspects, the functions of automation have associate possibilities of creating conflicts within their architectural components by either controlling or competing for network resources. This phenomenon could result in instability and conflicts [75] [12]. Hence, it becomes essential to introduce preventive measures to coordinate and manage autonomic functions within a single network which get executed concurrently. The network stability defines various conditions and focuses on improving the coordination of multiple concurrent processes in order to achieve efficient automation [76, 77] [78] [79].

3.1.5. Reinforcement Learning

In contradiction to the supervised and unsupervised learning strategies that consider labeled historic and unlabelled historical data, respectively, for generating predictive models, the reinforcement learning strategy considers software agent that interacts with the system, learns and creates optimal policy to achieve the given task in an automated manner [80, 81, 82, 83, 84]. The policies are optimized concerning the rewards and optimization function being used to ensure the software agent learn effectively.

3.1.6. Transfer Learning

The existing systems experience two major problems when adopting automation. Firstly, the availability of large amount of data and secondly the computational complexity of training the ML algorithm from scratch [85, 86, 87]. In order to cope up with both of these issues, transfer learning appears to be an effective approach. It helps to reduce the computational complexity in terms of training and the need for large amounts of data availability. This can be further achieved by leveraging the optimized weights of pre-trained networks.

3.2. Related Work aimed at achieving automation in ZSM

The network management automation problem in 5G systems has been gaining attention from both the standardization organization and the researchers [10]. An E2E automated network and service management system are vital to meet the 5G system performance requirements. In this regard, an industry specification group (ISG) for zero-touch service and network management (ZSM) was established by ETSI in 2017 [64]. The primary motive of this ISG specific to ZSM is to develop a reference architecture for an E2E service and network for automation and management of future and emerging networks. The automation term in the present era is intertwined with artificial intelligence, which leverages the characteristics of big data analytics and ML to automate the networks. A study in [10] predicted that the investment in AI-based network management systems would increase from 23 million dollars to 7.4 billion dollars by 2025, accordingly. Below are some of the studies that use zero-touch networks for the automation or standardization of communication systems discussed and well summarized in Table 3.

Fadlullah *et al.* [69] conducted a survey on the implications of deep learning in traffic control research, which concluded that the deep learning networks yield better performance on various prediction and classification tasks for routing strategies in comparison to the conventional methods. Martin et al. [71] proposed an AI-based framework for allocating network resources and is capable of self-healing, self-optimization, and self-configuration. They suggested that the proposed framework could adapt to the media service demand to increase the quality of user experience. Experimental results revealed that the AI-based framework achieves better scaling and resource efficiency than the conventional methods.

Calabrese et al. [80] proposed an autonomous learning architecture using reinforcement learning for radio resource management tasks. Their study concluded that the autonomous learning architecture could significantly reduce the operating and capital expenditure as a continual learning strategy would automatically adapt to new nodes and dynamic wireless environment in comparison to the existing rule-based radio resource management. Al-Tolppa et al. [85] proposed using case-based reasoning to detect anomalies for seal-healing of 5G radio access networks and diagnosis solutions. Experimental results showed that the case-based reasoning method was more resilient to anomalies than the existing approaches. Vilalta et al. [88] provided the development and design of network slice manager in the context of ZSM. The study suggested that the designed component can align with 3GPP, NFV, and ETSI models. Fernandez-Palacios et al. [89] performed a cost analysis under the EU PASSION project on sliceable bandwidth variable transponders based architectures in comparison to IP over Dense Wavelength Division Multiplexing (DWDM) networks using non-sliceable transponders. They concluded that the implementation of the said transponders in the context of ZSM, 29% and 42% savings could be achieved for OPEX and CAPEX scenarios. Rojas et al. [76] proposed a zero-touch coordination framework based on optimization techniques and ML algorithms to improve the coordination among self-organized network functions. Their study concluded that the proposed framework could multiple functions such as mobility robustness optimization and mobility load balancing, which can be executed simultaneously without any degradation in terms of performance. Boskov et al. [90]

Table 3: Analysis of Recent literature work towards A2A

Automation Techniques	**Application**	**Limitations**
Network Governance [3-4] [12,14]	- Traffic Control, Routing & Management - Network Resource Allocation - Self-Organized Network Functions	**- Lack of availability of the training data:** This leads to average desired performance. **-Most edge devices are resource constrained:** Therefore, handling computational expensive methods is a challenging task **- Increasing number of cybersecurity attacks:** Therefore, security remains one of the major concerns in communication systems.
Reinforcement Learning [5], [13], [24], [25]	-Radio and Network Slice Resource Management -Dynamic changes in 5G Networks -Fault Prediction	**-Large computational overhead in the training phase:** Therefore, designing less computational complex system is a challenging task. **-Topologically** & **transitionally scalable system design:** With the advancement in communication technologies and increasing IoT device users, this is necessity.
Intent-based Approaches [11], [15], [19]	-Self Healing Radio Access Network -Heterogeneous IoT Devices -Holographic Immersive Network Management -Network Slicing and Capacity Allocation	**-Managing the compatibility of devices used in the network:** This is due to the fact that they might vary in terms of data modality, feature space, device units, sampling rate, and others. **-Security for systems adopting intent-based approaches:** With the increasing number of cybersecurity attacks in recent years, security remains one of the major concerns.
Transfer Learning [6]	-Self Healing Radio Access Network	**-Handling computational expensive methods:** ZSM focuses on real-time processing that requires the computational complexity to be reduced without or with minimal impact on service performance **-Prone to the attribute-inference, label-inference,** & **model inversion attacks:** Considering the increasing number and rapid evolution of cyber-attacks, transfer learning is prone to above issues.
Network Stability [10], [13], [17], [19]	-AutoScaling for Management and Control -Dynamic Changes in 5G -Security Management -Network Slicing and Capacity Allocation	**-Managing the data and network parameter storage:** Managing huge amounts of data and constantly being able to retrieve it when needed is one of the challenging tasks associated with this technique. **-Design of non-parametric modeling methods:** These methods can be generalized for heterogeneous devices while managing their compatibility with the service provisioning is still an ongoing issue.
Policy-Based [11], [15]	-Heterogeneous IoT Devices -Holographic Immersive Network Management	**-Managing the compatibility of devices used in the network:** This is due to the fact that they might vary in terms of data modality, feature space, device units, sampling rate, and others. **-Increasing number of cybersecurity attacks:** Security remains one of the major concerns for systems employing policy-based approaches. **-Topologically** & **transitionally scalable system design:** With the advancement in communication technologies and increasing IoT device users, this is necessity.

proposed Bluetooth-based zero-touch provisioning along with software-enabled access point to arrange the provisioning of heterogeneous IoT devices. Their method was compared with manual provisioning methods on the LOG-A-TEC testbed. The results show that the method based on zero-touch provisioning outperforms the manual one by a large margin. Qin et al. [91] used the support vector data description (a ML-based approach) to perform the outage detection. Their simulation results reveal that their method could efficiently detect the small cell outages and the better QoS performance compared to the existing outage compensation and detection algorithms. Arteaga et al. [77] proposed using Gaussian processes and Q-learning to map the delay and dynamic changes in 5G networks. Their simulations were carried out on virtual evolved packet core, and it showed that the Q-learning-based approach outperforms the existing threshold-based techniques by a fair margin. Alternatively, Alawe et al. [72] presented a combination of long-short term memory and deep neural networks for proactively predicting the number of resources along with the network traffic to manage and scale the core network, i.e., mobility and access management, resources in 5G systems. Their experimental results revealed that the use of ML approaches improves the

scalability based on the forecasting and reacts to the change in traffic with lower latency.

Finally, Sanchez-Navarro et al. [37] suggested modifying ZSMs reference architecture to accommodate real-time automated tasks. Their experiments revealed that their interface helps obtain 25 frames per second for 2138 devices in a topology. However, the limitation in terms of hardware prevents the architecture from going beyond this benchmark. Bonati et al. [92] proposed the CellOS based on the principles of ZSM for cellular network management and optimization. Their results revealed that the CellOS records improvement up to 29% , 84% , and 86% improvement on fairness, energy efficiency, and throughput compared to the existing SDN techniques. Bega et al. [12] proposed anticipatory capacity allocation framework AZTEC for NS on ZSM principles. Their results revealed that the AZTEC framework could help reduce management costs while adapting to traffic variations dynamically and achieving better performance for network resource assignment compared to the state-of-the-art approaches. Fiaidhi and Mohammad [93] proposed to include the parallelization / distributed computing component in ZSM architecture and highly emphasized to use of graphical processing units for such tasks. They suggested that the graphical processing units have played a vital role in deep learning applications to reduce computational complexity and do the same for zero-touch services. Benzaid and Talib [10] conducted a survey on AI-driven approaches for ZSM architecture while exploring its research directions and challenges in 5G systems. They explored some of the research projects working in the field of ZSM such as SELFNET [94], CogNet [95], and SLICENET [96], all of them are categorized as 5G phase I and II projects. They also listed out various projects which are actively participating in building applications by leveraging ZSM characteristics. They also conducted preliminary experiments on the effect of data size and training time concerning the two widely used deep learning frameworks (PyTorch and Keras). Their results revealed that as the size of the data increases, the Keras framework achieves better accuracy while the Pytorch framework takes less time to train. Rezazadeh et al. [83] proposed reinforcement learning-based NS control for ZSM. The method subsequently reduced energy consumption, latency, and initiation cost of VNF, concerning each slice. Shaghaghi et al. [84] also proposed deep reinforcement learning-based approach for proactive failure recovery in ZSM networks. The study considers each VNF as a state in the Markov process and optimizes the wrong decision penalty and resource cost using the proximal policy optimization method. The authors also use long short-term memory cells in the agent structure of reinforcement learning to predict the failure time dependency.

3.3. Summary

Based on the aforementioned literature review, it can be summarized that:

- The use of Network Governance, Reinforcement learning, and Intent-based systems have been explored extensively for network resource management and self-organized network functions.
- Most of the works are focused on computational optimization, detection performance, NS, and resource management.
- The availability of training data is still a challenge for which transfer learning approach needs to be explored more.
- Moving forward to 6G networks, dealing with heterogeneous devices, data, and feature space is a challenge that needs to be explored concerning network governance and reinforcement learning.
- Scalability, security, and computational complexity are still the top most challenges in ZSM.
- In its entirety, the relevant literature is extremely limited to the context of achieving the goal of zero trouble networks. The new approaches such as federated learning with optimization algorithms such as Haris hawk [97] can be explored.

4. Cross-domain E2E Service Lifecycle Management

Automation of network management and service deployment has become essential for digital service providers to provide services with speed and efficiency [10]. Network management and cloud resource management should use digital service life cycle management systems to automate their service delivery completely. The goal of ZSM is to provide cross-domain E2E services that automate all operational activities such as deployment, configuration, assurance, delivery, and customization. The E2E service management domain manages and coordinates customer services as well as E2E services across domains [98]. The E2E service management domain reduces overall service complexity, allowing E2E management, domain management to operate autonomously. The ZSM architecture separates operational information from management applications, provides reliable data access, and provides cross-domain data services for the use of service intelligence, and network management [99]. The architecture is intended to endorse closed-loop automation for service and network management by utilizing automated decision techniques constrained by guidelines and regulations. Cross-domain data services allow:

1. Management data storage.
2. Sharing management information across domains with authenticated consumers.
3. Supporting big data analysis.
4. Providing data and intelligence services to eliminate routing misconfigurations and achieve desired service quality.

The E2E service management domain performs several services such as intelligence services, collection services, analytical services, orchestration services, control services, and delivery of various management services through service interfaces.

Each domain in ZSM is comprised of functional components that carry out specific tasks and highlight management services by utilizing service interfaces. Few services are internal, and only authorized domain functional components have access to them. [100]. Certain services exist outside of the domain and can be accessed by authorized functional components [101]. The E2E service management domain offers a variety of services, as shown in Fig. 3.

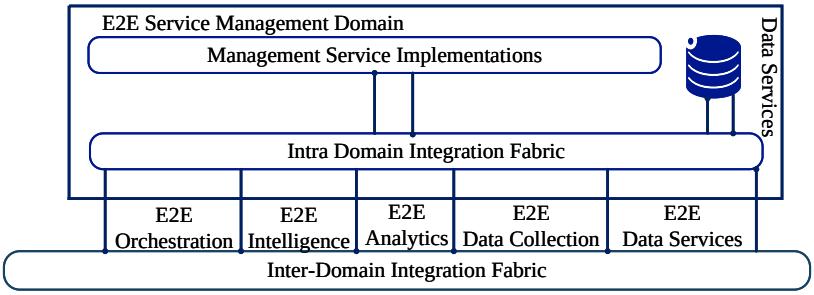

Figure 3: E2E service management domain [20].

The E2E service utilises orchestration to communicate different domains. The separation of management domains from the E2E service management domain significantly reduces complexity of the network. Data services enable data access and cross-domain data exposure by separating data storage and data processing. Every management domain, including the E2E service, delivers a variety of management services like collection services, analytics services, orchestration services, intelligence services through service interfaces. Certain services are only available and consumed within the domain through the intra-domain connection network. However, the inter-domain connection network enables cross-domain service exposure. Management services are accessible and utilized using the request-response or publish-subscribe models [101]. Fig. 4 illustrates the management processes during the E2E service lifecycle.

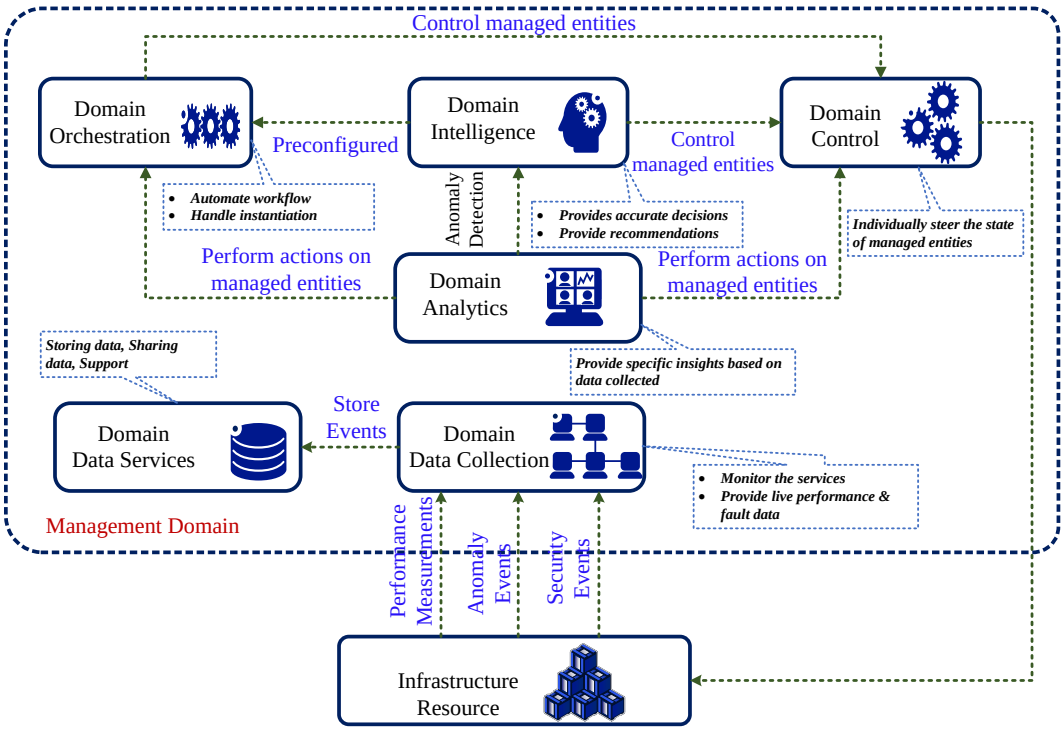

Figure 4: E2E management domain high-level architecture.

The ZSM architecture represents a collection of management services that various management functions can access. E2E Services are as fallows:

1. *E2E service data collection:* Allows the collection of live data while providing features for storing the collected data. It also provides services for reporting the E2E performance data.
2. *E2E service analytics:* Involves the process of collecting and analysing data in order to improve services enhancing customer experience. Provides some of the following analytic services:
   (a) E2E anomaly detection.
   (b) E2E service condition detection.
3. *E2E service intelligence:* Improves decision-making, prediction abilities, and action planning. Provides some of the following intelligence services:
   (a) AI management model.
   (b) AI training data management.
4. *E2E service orchestration:* Executes operational and functional processes, as well as creating, designing, and providing E2E services. Provides some of the following orchestration services:
   (a) Feasibility check service.
   (b) Managed services catalogue management service.
   (c) E2E testing service.

4.1. Different Aspects on E2E Service Life cycle Management

E2E service life cycle management is responsible for E2E services throughout their life cycle, interacting with management domains and domain services [102]. To manage the E2E service life cycle, several processes are used, which are divided into three categories: Service on-boarding, Service fulfilment and Service assurance [20]. Fig. 5 illustrates the management processes during the E2E service life cycle.

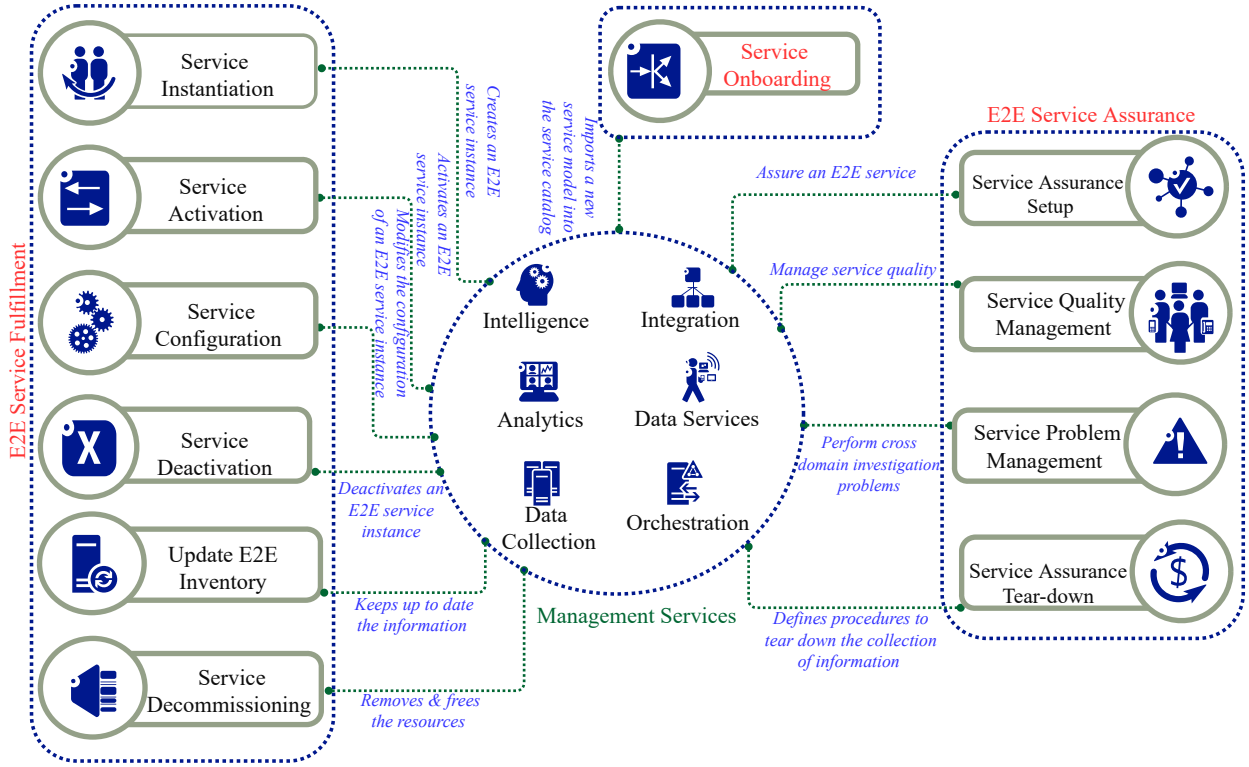

Figure 5: Management processes throughout the E2E service lifecycle.

Service on-boarding: The E2E service management domain performs service on-boarding to acquire E2E services from service design. The on-boarding process adds a new service model to the E2E service management domains service catalogue. on-boarding may also include the creation of a service template, which enables the service model to be parameterized whenever a concurrent service instance is needed [100]. Some of the management services involved are **E2E service orchestration**, which controls service models, and maintains services catalogue. **Domain orchestration**, which automatically sends out catalogue change alerts and requests missing service catalogue entries. Some of the additional management services that are used include **ZSM Integration Fabric**, which handles subscriptions, provides data, and receives data. **ZSM Data Services**, which stores data and provides data persistence services.

Service Fulfilment: The E2E service management domain manages E2E service instances from initiation to completion through the service fulfilment. The service fulfillment checks for service feasibility using feasibility check service, configures services, and tests them. The E2E service model must be onboarded before the service fulfillment process can begin [10]. The E2E service management domain accomplishes the following processes to deliver E2E service instances from creation to termination.

1. *Service Instantiation:* Requests the domain service instances to generate an E2E service instance. It checks the feasibility of the service, configures the service, and tests it. Some of the management services involved are **E2E service orchestration**, which manage service life cycle, provides E2E service orchestration service. **Domain orchestration**, which helps in checking feasibility, managing

service life cycle, configuring notifications, managing test specifications, providing test notifications, and testing service.

2. *Service Activation:* An E2E service instance is activated when a service activation is performed using Domain Orchestration Service. The service instance will provide services after it has been activated. The E2E service management domain stores information about the most current status of service instances [103]. If the domain service instance does not get activated immediately, the services are activated by the management domain. Furthermore, the management domain may implement changes such as resource scaling or reconfiguration. Some of the management services involved are **E2E service orchestration**, which manages the service life cycle and delivers E2E service orchestration service.

3. *Service configuration:* The E2E service management domain makes a request to the domain orchestration service to modify the configuration of one or more affected domain service instances, which in turn modifies the configuration of an E2E service instance [35]. Some of the management services involved are **E2E service orchestration**, which manages the service life cycle. **Domain orchestration**, configures the domain service. Some of the additional management services that are used include **ZSM Data Services**, which stores data and provides data persistence services.

4. *Service deactivation:* This procedure deactivates an E2E service instance using "Domain Orchestration Service"; once the service is deactivated, an E2E service instance cannot deliver its services. The deactivation request is handled by the management domain. The management domain does not deactivate service instances if they are used by some other E2E service instances [50]. The management domain may make changes by re-configuring the resources to indicate that the deactivated service instance is no longer using the resources. Some of the management services involved are **E2E service orchestration**, which manages the service life cycle. **Domain orchestration**, which deactivates and configures the managed service. Some of the additional management services that are used include **ZSM Data Services**, which stores data and provides data persistence services.

5. *Service decommissioning:* This procedure removes an E2E service instance and frees all of its resources. The E2E service management domain requests domain orchestration service to remove the service. After terminating the domain service instance, the management domain may make changes by re-configuring the resources to notify that the terminated service is no longer utilising the resources. Some of the management services involved are **E2E service orchestration**, which manages the service life cycle. **Domain orchestration**, which removes and configures the service's notifications. Some of the additional management services that are used include **ZSM Data Services**, which stores data and provides data persistence services.

6. *Update E2E inventory:* This procedure maintains the most up-to-date information about the resources and domain service instances managed by E2E service management. The E2E service management domain keeps track of all internal events and receives notifications from the management domains. The E2E service management domain maintains the corresponding changes in its inventory whenever an event occurs. Some of the management services included **Domain orchestration**, which provides a query inventory of available resources as well as notifications about lifecycle changes.

Service assurance: This procedure ensures that the E2E service meets its service level requirements. If the E2E service management domain is unable to resolve a service quality issue or if action is needed, the problem is escalated to the ZSM framework consumer through the notification of a service quality assurance

violation [61]. The E2E service management domain accomplishes the following processes to deliver E2E service assurance.

1. *Service assurance set-up:* The E2E service management domain establishes streams in the integration fabric by which information is transmitted via the "Management communication service." E2E service management domain configures performance monitoring and creates performance events for the service instances using the "Performance events service." The security events service monitors the security-related events of the services that are produced.

2. *Service quality management:* This procedure ensures that the E2E service instance meets the service level quality requirements and performs cross-domain investigation of quality control issues. If the E2E service management domain is unable to resolve a service quality issue, the issue is escalated to the ZSM framework.

3. *Service problem management:* This procedure ensures that the E2E service instance is error-free and conflict-free. If the E2E service management domain cannot resolve a problem, it is escalated to the ZSM framework.

4. *Service assurance tear-down:* This procedure tears down the information related to domain service instances that have been terminated or deactivated by their management domains. The tear-down occurs when a management domain decommissions or deactivates a service instance.

4.2. Existing Approaches to Accomplish Cross-domain E2E Services

5G mobile networks are being evolved to fulfill the challenges of a fully connected society, with the primary goal of providing end-users with exceptional mobile services via high speed and low latency. Future advancements and efficiency improvements are still required to design a 5G system capable of meeting the demanding requirements. Building, operating, and maintaining new inventions is challenging due to their novelty and lack of prior expertise in incorporating them. The work in [103] presents a federated-oriented, standards-based platform for transparent interoperability that employs a novel orchestration approach. The primary goal of this research is to solve the challenges of cross-domain slice orchestration. 5G-VINNI is a significant cross-domain E2E system that offers 5G features for sophisticated vertical experimentation across multiple domains. 5G-VINNI delivers a 5G-ready E2E facility with various operators and telecommunications equipment. The ability to manage autonomously is essential for Zerotouch Networks to deliver optimal services and operate use cases by 5G standards. More interestingly, in [104], the authors propose the Monitoring Model Generator (MMG) feature in ETSI ZSM for generating service monitoring templates. MMG employs a new approach in which service deployment models and standard information models acts as inputs to produce a monitoring template known as the service monitoring model, a monitoring template built with an ontology framework focused on there source description framework vocabulary. In [37], the authors proposed an innovative visualization-based immersive model that allows network admins to communicate with a ZTM system in a conventional manner. The main goal of this work is to create a GUI with E2E debugging features so that the operator can visualise and predict the autonomous systems tendencies. In [10], the authors suggested a framework for domain operators to highlight their features and functionality in relation to cross-domain E2E services. Capability orchestration is recommended as a technique and investigated to understand the process involved in communicating business objectives using capability orchestration methods. The primary objective of this work is to provide an agile methodology for IT professionals and operators to monetize domain resources. Also, the study in [105] proposed a generic intent-based system for orchestrating and managing network life-cycles across domains. The primary goal of this work is to provide cross-domain E2E service orchestration via multiple domains.

The concept of network slicing is essential in 5G and beyond. Network slicing enables the deployment of various applications and services on virtualized resources. Creating a scalable process for orchestration of E2E network slices usually involves proper planning and extremely reliable algorithms. In [98], the authors proposed a E2E Network Slicing Orchestration System (NSOS) and a Dynamic Auto-Scaling Algorithm (DASA). DASA mechanism provide proactive and reactive resource functionality. DASA works based on

the queuing model that comprises of an open network of G/G/m queues. The proposed work was carried out by introducing a dynamic scaling algorithm that allows maximization of the orchestration in E2E global network slices depending on the resources thereby establishing an orchestration time policy. Table. 4 summaries the existing approaches to accomplish cross-domain E2E services.

Table 4: Existing approaches to accomplish cross-domain E2E services.

Ref.	Approach	Features
[103]	Federated-oriented, standards-based platform for transparent interoperability that employs a novel orchestration approach.	5G-VINNI is a significant cross-domain E2E system that offers 5G features for sophisticated vertical experimentation across multiple domains. 5G-VINNI delivers a 5G-ready E2E facility with various operators and telecommunications equipment.
[104]	MMG feature in ETSI ZSM for generating service monitoring templates.	MMG employs a new approach in which service deployment models and standard information models acts as inputs to produce a monitoring template.
[37]	Proposed visualization-based immersive model that allows network admins to communicate with a ZTM system.	Create a GUI with E2E debugging features so that the operator can visualise and predict the autonomous systems tendencies.
[10]	Suggested a framework for domain operators to highlight their features and functionality in relation to cross-domain E2E services.	Provide an agile way for IT professionals and operators to monetize domain resources.
[105]	Proposed a generic intent-based system for orchestrating and managing network life-cycles across domains.	Provide cross-domain E2E service orchestration via multiple domains.
[98]	Proposed a E2E Network Slicing Orchestration System and a Dynamic Auto-Scaling Algorithm.	Provides a dynamic scaling algorithm that allows to maximise the orchestration of E2E global network slices depending on the resources and establish an orchestration time policy.

4.3. Summary

The summary of cross-domain E2E service life cycle management is as follows:

- The cross-domain E2E service management contributes in providing services in various domains namely intelligence services, collection services, analytical services, orchestration services, control services and delivery of management services in versatile verticals.
- The cross-domain E2E services aids in taking real time decisions, enhances prediction abilities and also enables effective action planning.
- The cross-domain E2E services provides intelligence services in association with orchestration services that help to improve the configuration required to maintain desired level of service quality.
- The cross-domain E2E service life cycle is managed by three processes namely on-boarding process, fulfilment process and assurance process. The on-boarding process adds a new service model to the E2E service management domains service catalogue. The fulfilment processes enables a service instance based on the on-boarded service model, configures the service instance, activates the same to make it operational and finally terminates it at the end of the process. The assurance processes ensures that a service is free of faults and it renders optimal quality service management.

5. Security Aspects

To ensure privacy preservation and security, E2E security management is crucial to establish clear identities. The threats to the network have increased rapidly and continuous evolution in association with the

rise number of connected devices have also been observed[106]. The major security challenges faced by ZSM and the potential counterattack mechanisms are discussed in this section.

The security threats related to ZSM can be categorized as violation threats, deliberate threats, accidental threats. Fig. 6 illustrates major threats related to ZSM.

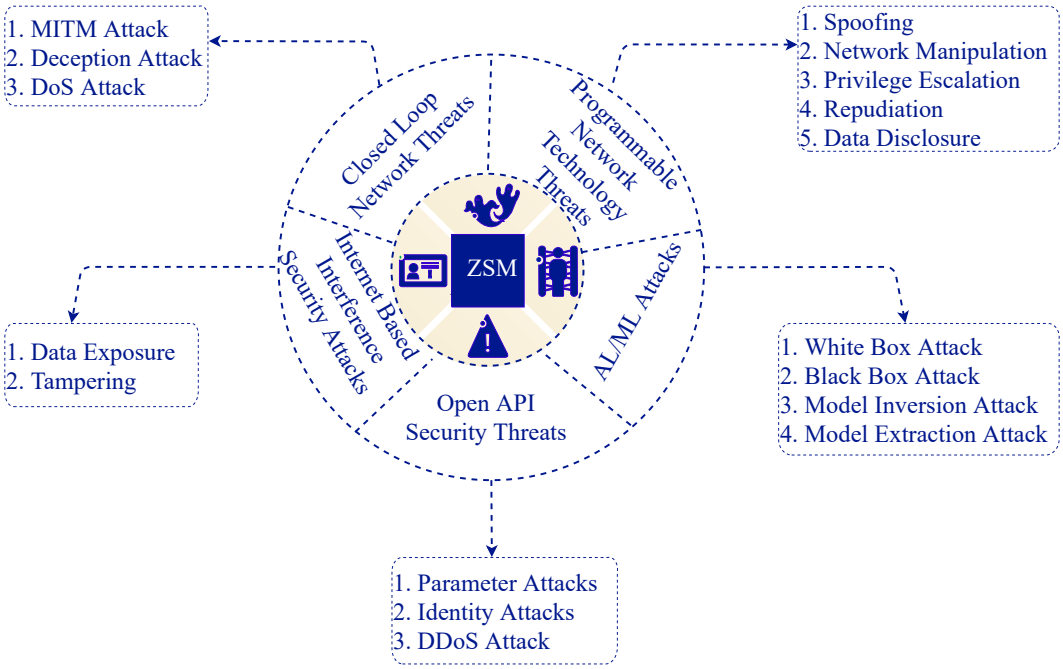

Figure 6: Possible threats and attacks on ZSM.

5.1. ML/AI-based Attacks

Implementing ML approaches on network and service management results in substantial enhancements in service efficacy, performance, and time management, enabling new business models to emerge. ML/AI approaches are predominantly used for intelligent network management and activity capabilities. In addition, they also support Traffic management, forecast, mobility assessment, and resource distribution. Network security has recently gained immense momentum [107] since if the vulnerability around the usage of AI/ML techniques is not resolved, its use in next-generation network management may be dampened. Undoubtedly, the use of AI/ML and other data analytic technologies have initiated new attack vectors. As an example, model inversion attacks and model extraction attacks have emerged recently that target ML as a Service [108, 109, 110]. In model inversion attacks, the training data is reconstructed from the model parameters that can be used to extract private and sensitive data. Model extraction attacks use model parameters extracted by querying the model. It has also been identified that ML approaches are susceptible to a variety of interventions [107] that exploit both the training phase (i.e., poisoning attacks) and the testing phase (i.e., evasion attacks).

Based on the attacker's knowledge, attacks on ML can be classified into two categories, the white-box, and black-box attacks [111].

White-box attack. In case of a white box attack, the intruder has a full understanding of the classification model. The intruder is completely aware of the training algorithm and can thus exploit the training data distribution and the parameters of the entire trained model architecture. [112].

Black-box attack. On the contrary, the attackers do not know the classification model, its algorithm, training data, and the model architecture [113]. The black box attack analyses the model's vulnerability using knowledge about its settings or previous inputs. Black box attacks can be categorized as strict black-box attacks, Non-adaptive & adaptive black-box attacks. In non-adaptive black box attack, only the distribution of the training dataset can be accessed by the attacker while in adaptive black box attack the attacker will not have access to the distribution of the training dataset, however the attacker will have access to the training model. In strict black-box attack the attacker does not have access to the distribution of the training dataset and cannot modify the input query to observe the output of the model. In addition, the attacker will not be able to change the input query in order to observe the model's results [114].

5.2. Open API Security Threats

APIs (Application Programming Interfaces) is a technology used for incorporating web-based applications[115]. APIs are an extremely critical component of the ZSM architecture, enabling communication that interfaces between its components and services. Parameter attacks such as Script insertions, SQL injections, buffer overflow attacks along with Man in the middle attack, identity attacks, and denial of service (DoS) are possible API-based attacks working against the ZSM system[116].

5.2.1. Parameter Attacks

It takes advantage of data that is transmitted through an API, which includes the query parameters, HTTP headers, uniform resource locator, and post content[117]. The following are possible API parameter attacks.

Script insertions. This type of attack takes advantage of systems that interpret the submitted parameter content as a script.

SQL injections. This is a query language-based attack in which parameters are designed to load a particular input into a database query. The query is tampered with to alter the intent of an underlying SQL template.

Buffer overflow attacks. These attacks are triggered by data beyond the intended types or ranges. It results in a system crash, thereby providing access to memory spaces.

Identity Attacks. These attacks try to gain access to a target API using a list of previously compromised passwords, stolen credentials, or tokens. It feeds large quantities of random data into a framework to find vulnerabilities[118].

Denial of Service Attacks. These attacks overwhelm essential API resources by sending large traffic volumes from multiple sources and interrupting access to these services.

Application and Data Attacks. These attacks incorporate data breach, data deletion or modification, code injection, and script disruption.

5.3. Intent-based Security Threats

The intent-based interfaces use network orchestration, AI, and ML to automate administrative capabilities[119]. The goal is to minimize manual associations. The potential threats related are data exposure, unusual behavior, and inappropriate configurations.

Data Exposure. Automation will expose data regarding the application's interests such as communicating with associates, advertising content, and managing traffic. Consequently, an unauthorized party intercepts such information endangering system objectives leading to the launch of other attacks.

Tampering. The intruder makes physical changes to an interface or a contact connection. As a consequence, disconnecting or modifying the physical connection occurs along with modification of the transmitted data.

5.4. Automated Closed-Loop Network based Security Threats

Closed-loop automation(CLA) is a continuous process that tracks, evaluates, and assesses real-time network traffic enhancing end-user Quality of Experience. External CLA capabilities are required to deal with the expanding threat in 6G technologies[35, 120]. CLA security mechanisms have the potential to automatically detect threats such as DOS, Man In The Middle attack (MITM), Deception attack, unknown threats and quickly mitigate them using ML and AI.

MITM Attack. When an intruder intercepts messages between two parties to remotely eavesdrop or manipulate traffic, it is known as a MITM attack. It captures user credentials, personal information, and spies on users interrupting their messages, leading to data corruption.

Deception Attacks. Deception is an exchange of information between two entities - a deceiver and a target. In such attacks, the deceiver effectively convinces the target to accept an incorrect version of the truth as fact and manipulates the target to behave in a way that benefits the deceiver.

5.5. Threats due to Programmable Network Technologies

SDN and NFV technologies are used to create a programmable networking solution. When users have programmatic access to SDN, the risks increase. These threats are predominant in situations wherein the users are forced to "trust" and rely on third-party applications or standard-based solutions for network access. Also, in the absence of appropriate isolation, the control information and network element management get exploited to attacks such as Network Manipulation, ARP Spoofing Attack, and others. Functional Virtualization needs to support an infrastructure that is independent of hardware. NFV is prone to generic virtualization threats, generic networking threats, and virtualization of technology threats[121]. VNFs are vulnerable to design, implementation, and configuration defects, leading to inappropriate monitoring of data that misleads the service intelligence and E2E analytics in ZSM.

5.6. Possible Threats on ZSM Framework Architecture

The E2E service intelligence offered by ZSM facilitates decision-making and also helps in predicting capabilities. Information from data services and domain data collection services are used to make important decisions. As a result, an intruder may generate inputs to deceive the ML algorithm used by the E2E intelligence services leading to incorrect assumptions or conclusions, resulting in decreased efficiency, financial loss, and endangering of service level agreement fulfillment and security guarantees. APIs are used extensively during the Services provisioning, governance, orchestration, and monitoring in the ZSM, making them the possible ideal target for intruders. An attacker can potentially access or interfere with ZSM's services by using insecure APIs. Data loss, theft of personal information, server compromise, and service outage are all possible outcomes of API-based attacks.

One of the core principles of the ZSM architecture is intent-based interfaces. A registered consumer may use the ZSM domain orchestration service to create, modify, and terminate domain-level network services. An attacker may try to use the orchestration service from a compromised consumer and tamper with the interfaces. ZSM architecture supports closed-loop control automation of domain data collection. An attacker may initiate a deception attack by sending a fabricated fault event to the ZSM domain data collection interface claiming VNF as faulty.

The fault event service in a domain data collection process publishes fake fault cases. It is accepted by the domain intelligence services as part of the closed-loop service at the domain level and responds to the attacker. If the attacker successfully hijacks the response or reroutes the traffic via an attacker-controlled switch, the man-in-the-middle attack is performed. The ZSM architecture is built on a foundation of the programmable network approach by integrating with SDN and NFV technologies. The attacker uses possible attacks like tampering, spoofing, information disclosure, repudiation, DoS attack, and privilege escalation on SDN, used by the ZSM framework. The attacker can also compromise VNFs providing inaccurate monitoring data thereby misleading the analytics and intelligence services of the ZSM framework.

5.7. Existing Works on ZSM Security Threats and Related Mitigation Mechanisms

Deep Learning (DL) has been used as tool to improve the security of ZSM systems. Q.Liu et al. in [112], used DL-based channel state information (CSI) to demonstrate the impact of an adversarial white-box attack on a DL-based communication system. The study revealed the negative impact of the adversarial attack by evaluating deep learning-based CSI feedback performance. In addition, a jamming attack was also launched for comparison and found that the jamming attack could be prevented by using certain precautions. The study had shortcomings in terms of dealing with the adversarial interruption in ultra-secure communication systems. A new iterative gradient attack (IGA) model based on gradient information in the trained graph autoencoder (GAE) model in [107] was used to solve the link prediction adversarial attack problem. Extensive tests on a wide range of real-world graphs revealed that most deep models and state-of-the-art relation prediction algorithms are vulnerable to adversarial attacks. This study also proposed techniques for making the adversarial attack more feasible in practice and found that the algorithmic complexity of IGA increases as the graph scale grows larger. The study had limitations in addressing algorithmic complexity reduction on larger graphs, and mitigation strategies for attacks are not clearly defined. A deep learning-based adversarial attack to launch over the air spectrum poisoning attacks that target the spectrum sensing period and compromise the transmitter's input data during the test and training phases was proposed in [122]. They focused on countering these attacks, but the research had limitations over other mediums of data transmission.

The emergence and mitigation of attacks have always been a part of network security. H. Yan et al.[113] introduced an adaptive query-flooding parameter duplication (QPD) attack in which the attacker uses black-box access to infer model information. They also developed a defense strategy using DP called monitoring-based differential privacy (MDP) against this new attack. There is a serious limitation on the defense of MDP over other kinds of subversion attacks like evasion and poison attacks. DIAVA[115], a new traffic-based SQL injection attack has an identification and vulnerability analysis system that can alert users while assisting in real-time threat evaluation of data loss as a result of SQL injection. The research had drawbacks relevant to evaluation of large-scale real-time susceptibility to parameter attacks. CuRTAIL, an E2E computing architecture used a series of complementary but disjoint modular redundancies to validate the validity of input samples to characterize and thwart possible adversarial attacks and dramatically improve the reliability of a victim DL model. To achieve optimum throughput, it is fully paralleled through multiple hardware settings. The authors [123] suggested API was seen to be effective in a wide range of applications. An anomaly-based intrusion detection framework was proposed[124] to detect and mitigate new forms of DDoS attack in real-time. The proposed intrusion detection system can detect and mitigate stealthy DDoS attacks, even with very small attack sizes per source. The research is restricted to complex networks.

For session-initiation-protocol-based next-generation networks, Azad et al.[125] implemented a modern self-enforcing authentication protocol. Instead of using a Public Key Infrastructure or a trustworthy third-party scheme, this protocol uses a low-entropy mutual password. The proposed system appeared to be competitive against several attacks being still constrained in real-world scenarios and attacks. A novel auto-scaling mechanism based on multiple optimization algorithms [119] was proposed in compliance with ZSM and converged cross stratum orchestration. Their study revealed the fact that the auto-scaling mechanism supports Telco operators to manage and control their network in an automated manner. Carrozzo et al. [126] expanded the concept of AI-driven ZSM to security and trust domain in 5G networks. They leveraged the characteristics of blockchain technology such as smart contracts and distributed ledger technologies to enhance the security amongst non-trusted parties. A hypothetical architecture for E2E security management in 5G networks based on ZSM principles was proposed in [127]. Their hypothetical framework leverages the characteristics of distributed ledgers, ML, and a trusted execution environment to achieve the desired security levels and meet the requirements of security service level agreements.

5.8. Summary

Based on the aforementioned literature review which emphasized potential risks to ZSM, as well as mitigating strategies which are shown in Table 5. The following section can be briefly outlined as follows:

Table 5: Possible threats on ZSM

Possible threats on ZSM							
Threat	AI and ML	Open API	Intent based interface	Closed-Loop Networked Automation	Programmable Network	ZSM framework architecture	Possible mitigation mechanisms of various threats related to ZSM
Adversarial attacks	H	H	M	M	H	H	Defense GAN's, Defensive distillation, Adversarial training, Concept drift, Input validation [128]
model extraction attacks	H	H	L	L	M	H	Control information provision [108]
model Inversion attacks	H	H	L	H	H	H	Adding noise to ML prediction [108]
Script insertions	L	H	M	M	H	M	Input validation [128]
SQL injections	L	H	M	M	H	M	Input validation [128]
Buffer overflow attacks	L	H	M	M	H	M	Input validation [128]
identity attacks	M	H	H	M	H	H	Secure communication[125]
Application attacks	L	H	H	M	H	H	Authentication control[125]
Data attacks	M	M	H	L	L	H	Authorization control[125]
DDoS attacks	H	H	H	H	H	H	Client throttling[124]
Data exposure	M	M	H	H	H	H	Authentication and Authorization control[129]
Tampering	M	M	H	H	H	H	Secure Communication [129]
Malformed Intent	M	M	H	M	M	M	Intent format validation [119]
Conflicting Intents	M	M	H	H	M	M	Conflicting Intents detection/resolution [119]
Dos Attack	H	H	H	H	H	H	Client throttling [124]
MITM attack	H	H	H	H	H	H	Secure Communication,Authentication and Authorization control [130]
Deception attacks	H	H	H	H	H	H	multi-factor authentication and enhanced access control[131]
Spoofing	H	H	H	H	H	H	Authentication control[132]
Privilege escalation	M	M	M	M	H	M	Authorization controls
Information disclosure	M	M	H	H	H	H	Secure communication

L Low Impact M Medium Impact H High Impact

- The potential security vulnerabilities on the ZSM framework include AI/ML-based attacks, open API security threats,intent-based security threats, closed-Loop networked automation security threats, and attacks due to the adoption of programmable network technologies.
- The use of best practices and mitigation steps can help in countering attacks and threats on ZSM.
- The up-to-date automated threat identification and mitigation mechanisms could aid in the automation

of security services in ZSM.

- Protection and mitigation updates must be given top priority, as the entire ZSM framework is based on it.
- The use of automated AI/ML, blockchain, and zero trust mechanisms strengthen ZSM's defenses against potential threats.
- Security automation and protection of programmable network technologies exist as challenges for the ZSM framework.
- The subsections discussed possible threats, mitigation mechanisms and also suggests the use of potential technologies like blockchain and zero trust mechanisms for security enhancement in the ZSM framework.

6. Standardization and Projects

ZSM is a prominent technology in the next generation of mobile networks, which has an extended project and landscape of standardization. This section presents the main standardization activities and research projects relevant to ZSM and 5G networks.[1]

6.1. Landscape of ZSM related Research Projects

6.1.1. 5GZORRO (2019-2022)

5GZORRO (Zero-touch security and trust for ubiquitous computing and connectivity in 5G networks) is an EU (European Union) funded H2020 project which aims at developing solutions for zero-touch service and security management of beyond 5G networks [133]. 5GZORRO project utilizes the distributed AI to realize cognitive network orchestration and service management with the help of blockchain/Distributed Ledger Technologies (DLT) and zero-touch service automation mechanisms. This approach can enable dynamic and flexible security and enhanced distributed trust within the 5G E2E service chains.

6.1.2. Inspire-5GPlus (2019-2022)

Intelligent Security Architecture for 5G and Beyond Networks (Inspire-5GPlus) is an EU-funded H2020 project which mainly aims at the advancement of 5G and Beyond networks security [134]. To achieve this aim, the INSPIRE-5Gplus project focuses on improving the security of 5G and beyond 5G mobile networks at different dimensions, i.e., overall vision and architecture, 5G applications and use cases also network management. The project will identify the critical risks and threats beyond 5G networks and develop innovative concepts for security management to mitigate these cybersecurity risks. Inspire-5GPlus has a particular focus on the security of the ZSM framework.

6.1.3. MonB5G (2019-2022)

MonB5G (Distributed management of Network Slices in beyond 5G) is an EU-funded H2020 project which aims at developing a multi-tier automated network management system for 5G and beyond networks with fault-tolerant capabilities [135]. MonB5G system considers energy efficiency and network security as the main features to orchestrate the network. Furthermore, it develops the methods to manage network slices to enable different novel network services in a zero-touch manner to realize adaptability. Thus, the MonB5G project develops a novel autonomic MANO framework based on data-driven AI-based mechanisms to enable zero-touch MANO in massive-scale NS for 5G and beyond networks.

[1]Please note that although there is a broad spectrum of standardization activities and research projects, we mainly focus on the major activities with a significant focus on ZSM.

6.1.4. 5G-VINNI (2018-2021)

The 5G-VINNI (Verticals Innovation Infrastructure) is an EU-funded H2020 project aiming to accelerate the adaptation of 5G networks and services in Europe by offering an E2E testing infrastructure [136]. It can ultimately reduce the entry barrier for new vertical industries to pilot 5G use cases. Therefore, the project focuses on developing a 5G infrastructure to deploy an E2E 5G facility. Furthermore, it can be used to do early demonstrations of 5G services, verify the 5G KPIs (Key Performance Indicators) of 5G services with practical implementations. Thus, 5G-VINNI supports the testing of different 5G and beyond concepts, including the ZSM.

6.1.5. Hexa-X (2021-2024)

Hexa-X (A flagship for B5G/6G vision and intelligent fabric of technology enablers connecting human, physical, and digital worlds) an EU-funded H2020 project which focuses on the realization of 6G wireless networks with explorative research (X) [137]. The vision of Hexa-X projects is to interconnect three worlds, i.e., digital, physical, and human, via 6G key enablers. In the ZSM domain, the Hexa-X project contributes to the evolution of ZSM architecture and interfaces for full network programmability and automated life cycle management. Hexa-X will also focus on developing beyond 5G PoC (Proof of Concept), demonstrating interfaces and interoperability of ZSM management plane functions based on project findings.

6.1.6. 6G Flagship (2018-2026)

The Academy of Finland funded 6G flagship project is focusing on three main goals, i.e., 1) Provide support to industry in finalization of 5G deployment and services, 2) Research and development of the key enabling technologies for 6G realization, and 3) Speed up digitalization in society via 5G and beyond 5G technologies [138]. The 6G flagship is organized into four main interrelated strategic research areas, i.e., wireless connectivity, device and circuit technology, distributed computing, service, and application to achieve these goals. In addition, the 6G flagship is also focusing on security aspects of the ZSM framework by utilizing AI and blockchain technologies. Moreover, the 6G flagship project cooperates with other EU-level projects such Hexa-X and Inspire-5GPlus in the ZSM domain.

6.1.7. Other related Open Source Projects

Several other open-source project initiatives such as OpenStack [139], Open Source MANO (OSM) [140], Open Network Automation Platform (ONAP) [141], Open Platform for NFV (OPNFV), and Open Platform for NFV (OPNFV) [142] are also quite relevant to realizing the ZSM framework and its deployment in various 5G and beyond use cases.

6.2. Landscape of ZSM Related Standards Developing Organizations (SDOs)

Different SDOs actively participate in the ZSM related standards. The following section presents the vital standardization activities from SDOs. Table. 6 summarizes the impact of different SDO activities of ZSM related technical aspects and technologies.

6.2.1. European Telecommunications Standards Institute

ESTI has a dedicated ZSM WG [143], which focuses on the full E2E network automation and management of services. The main aim of ESTI ZSM WG is to speed up the standardization of E2E ZSM architecture and deployment of ZSM based services.

In this regard, the ETSI ZSM group has released several specifications on ZSM as the following.

- **GS ZSM 001**: Potential scenarios and requirements of ZSM are explicitly specified [13].
- **GS ZSM 002**: Based on scenarios and requirements defined in ZSM 001, a set of architectural requirements are explained to design a reference architecture for ZSM [14].
- **GS ZSM 003**: ZSM solutions and interfaces to support automation and management of emerging technologies such as NS are specified [15].

Table 6: Contribution of ongoing research projects and SDO activities on ZSM

	Technical Aspects				Related Technologies				
	Architecture	Service Automation	E2E Service Life-cycle Management	Security	AI/ML	SDN/NFV	NS	Edge/Cloud Computing	Other Technologies
Research Projects									
5GZORRO	M	M	L	H	H	L	L	M	H
Inspire-5GPlus	M	M	M	H	H	M	H	H	H
MonB5G	H	M	M	L	H	M	H	M	L
5G-VINNI	L	M	M	L	H	H	H	H	M
Hexa-X	H	M	M	M	H	M	H	H	M
6G Flagship	H	M	M	H	H	H	H	H	H
Standards Developing Organizations (SDOs)									
ESTI	H	H	H	H	H	H	H	H	H
3GPP	M	H	M	M	H	H	H	M	M
ITU-T	H	M	M	M	H	M	M	M	M
TM Forum	M	H	H	L	M	M	H	M	L
ONF	M	M	M	M	M	H	M	M	L
GSMA	L	L	L	L	M	M	H	M	M
OASIS	L	M	L	L	M	M	M	H	M

L Low Coverage M Medium Coverage H High Coverage

- **GS ZSM 004**: This specification summarizes related activities of ZSM such as standards developing organizations, industry participants, and open sources initiatives [16].
- **GS ZSM 005**: This specification explores different means and solutions of ZSM towards a fully automated network, including intent-based services, network governance, network stability, and applications of AI techniques such as as as reinforcement learning and transfer learning [17].
- **GS ZSM 006**: This specification details a framework to promote the realization of different aspects

of ZSM from various stakeholders [18].

- **GS ZSM 007**: A detailed explanation of particular concepts in ZSM is provided in the ZSM 007 specification [19].
- **GS ZSM 008**: Cross-domain E2E service management activities, solutions, and challenges are described in this specification [20].
- **GS ZSM 009**: Key enablers and solutions for ZSM E2E services and use cases are specified [21].
- **GS ZSM 010**: Security threats and existing solutions related to ZSM are identified to ensure full automation of network operation and management [22].

6.2.2. 3rd Generation Partnership Project (3GPP)

3GPP Service and System Aspects Working Group 2 (SA2) and SA5 are working on developing the standards relevant to ZSM. The following actions in SA2 and SA5 can be identified as primarily related to ZSM realization in 5G and beyond networks.

A Network Data Analytics (NWDA) framework is proposed by 3GPP SA2 to automate the sharing of data analytics specific to network slices to support the 5G network automation [144]. In addition, new Service-Based Architecture (SBA) for 5G is proposed to enhance the agility of network slice deployment, enable service re-use and improve the flexibility of NS based on 5G services [145].

3GPP SA5 specifies the automatic collection of real-time performance data to detect the potential issues in virtualized network functions (VNFs) in 5G networks [146]. In addition, 3GPP SA5 defines requirements to automate fault management of 5G and beyond networks that comply with ZSM standards. 3GPP SA5 also specifies the automated network policy management framework for NFV scenarios 5G network [147, 148]. Finally, an Intent-Driven Management (IDM) service for 5G networks which can significantly reduce the complexity of automated network and service management is developed by 3GPP SA2. IDM service will enable the consumer to define desired intent for 5G network, and service [149].

6.2.3. International Telecommunication Union - Telecommunication (ITU-T)

Several activities in ITU-T have immediate relevance to realize the implementation of ZSM in 5G and beyond networks. ITU-T Study Group 13 establishes a new Focus Group on ML for Future Networks, including 5G (FG-ML5G). FG-ML5G focuses on applying ML for different aspects of 5G and beyond networks, such as network architectures, interfaces, radio spectrum, algorithms, and data format. Moreover, ITU-U specifies a framework to use ML in future networks [150]. This framework and specifications of using ML in a mobile network are essential to develop ZSM architecture and deploy ZSM based 5G networks.

6.2.4. TM Forum

TM Forum is developing the vision of Open Digital Architecture (ODA) [151] as an agile replacement for existing OSS/BSS (Operational Support System/Business Support System) architecture. More importantly, the proposed ODA is closely co-related with ZSM architecture. For instance, the ODA user guidelines to manage the NS systems are correlated with network slice management guidelines in ZSM. Both ODA and ZSM user guides focus on management network slices to support multiple and changing business models. Therefore, ODA development activity in TM Forum will complement the ZSM standardization to a certain extend.

6.2.5. Open Networking Foundation (ONF)

ONF specifies the Central Office Re-architected as a Datacentre (CORD) platform [152] which leverages SDN, NFV, and cloud computing technologies to build agile edge data centers networks. The CORD is an open, programmable, and agile platform that allows the MNOs (Mobile Network Operators) to deploy and test cloud-native innovative services. Moreover, ONF develops the data models and open-source software tools, which are helpful in deploy SDN-based networks, including 5G and beyond networks. Specially, these tools can also facilitate the convergence and federation in SDN, NFV and cloud computing technologies to

avoid needless fragmentation. ONF is also developing specifications of Intent-based Networking interfaces for SDN [153]. The above activities in ONF help the proper integration of ZSM in SDN-based networks, including 5G and beyond networks.

6.2.6. Global System for Mobile Communications Association (GSMA)

GSMA has initiated a Network Slicing Taskforce (NEST) project to enable interoperability and harmonize the slicing creation process across multiple operators. GSMA also defines a comprehensive set of service requirements on NS for different vertical industries, such as AR/VR, vehicular networks, smart grids, healthcare, Industry 4.0, public safety, and smart cities [154]. These activities complement the realization of ZSM for NS use cases.

6.2.7. Organization for the Advancement of Structured Information Standards (OASIS)

OASIS has the Topology and Orchestration Specification for Cloud Applications (TOSCA) technical committee which is conducting the standardization tasks related to ZSM realization. TOSCA defines the inter-operable network services description for novel cloud services to enable portability and automated management across multiple cloud providers [155, 156].

6.2.8. Other SDOs

In addition to the above SDOs, there are several other SDOs such as Broadband Forum (BBF), Internet Engineering Task Force /Internet Research Task Force (IETF/IRTF), TM Forum, MEF, are also focusing on the standard development for 5G and beyond networks which are useful in ZSM realization.

7. Lessons Learned and Future Research Directions

There exists prominent complexity in the operation and management of 5G networks and beyond which have accelerated the development of close loop automated networks and service management operations. The ZSM is considered as the future of next-generation management system. An overview of the lessons learned in various aspects of the ZSM framework, its open issues and the possible solutions are discussed in this section. Table. 7 provide a concise highlight of the same.

7.1. Architecture

7.1.1. Lessons Learnt and Open Issues

The major lessons learned from the ZSM architecture is its mistake in not including the third party as part of the architecture apart from the manufacturer and the owner. In this case, the customer acts as the third party. The ZSM solutions provide secure and effective solution mechanisms to ensure the device to owner connectivity through "late binding". In a typical situation, the owners fail to get the chance of touching the device's delivery chain or its supply, and late binding becomes effective. It is observed that whenever the customers are perceived as service providers being excluded from the on-boarding process of the devices and the role is taken over by owners, issues evolve. The network in such instances fails to provide any solutions for the owner to securely achieve automated "device to location", "device to subscription", and "device to the premise" bindings. The ZSM solutions are focused on achieving zero-touch experiences from the owner's side alone. If the customer gets involved with the owner being the service provider, the customer's zero-touch experience is ignored. Basically service providers fail to design a mechanism for achieving the binding without critical review and standardization. [10].

7.1.2. Possible Solutions

Firstly, active involvement of customer or owner through manual intervention could close the device-to-premises critical gap. Also, the customer policies could be manually bound to each device, mapping the same with some known ID of the service subscriber premises. Thus, the binding and on-boarding task could be securely automated. The device to premises binding could be eliminated entirely, which would also reduce plausible threats in the deployed services [10].

Table 7: ZSM - Various lessons learned and future research directions.

ZSM Domain	Lessons Learned	Open Issues	Solutions
Architecture	∘ Owners fail to touch device's delivery chain. ∘ Customers perceived as service providers, owners takeover. ∘ Owners fail to achieve automated "device to location", "device to subscription", and "device to premise" bindings. ∘ Focused on achieving zero touch experiences from the owners side alone.	∘ Non inclusion of customers in the on-boarding process. ∘ Exclusion of the customer side zero touch experiences. ∘ Service providers inability to design a mechanism for achieving the binding without critical review and standardization.	∘ Active involvement of customer or owner through manual intervention. ∘ Closing of the device-to-premises binding gap. ∘ Customer policies to be manually binded to each device using known ID of the service subscriber premises. ∘ Binding and on-boarding task could be securely automated. ∘ Elimination of device to premises binding.
Automation	∘ Automation challenges exist in five functional areas namely business language based, translation, policy, reasoning and configuration enforcement. ∘ AFs compete with each other. ∘ Intent based approach used as means of automation. ∘ Dependence on the loop structure to perform their basic operation. ∘ Common closed control loops exist in MAPE-K, MRACL and OODA.	∘ Complexity of the networks and services. ∘ Need for a business language in case of network governance. ∘ Exploitation of the concept of reasoning in governance. ∘ Requirement of policies for optimal configuration of service selection and translation from business level to low level policies.	∘ Transformation of networks into programmable, software-oriented, service based and intricately managed architectures. ∘ Use of appropriate business rules and solutions to connect high level goals and network resources for human friendly governance interface. ∘ Guidance for infrastructure behaviours to be provided during process of service view. ∘ Operator to be guided for smooth functioning of the autonomic network
E2E LC Management	∘ E2E services of ZSM run the closed loops in the service management. ∘ Service-specific predictions based on service demands, decision making and execution processes. ∘ ML-based decision making, possibilities of data manipulation, leading to erroneous results being generated from the ML model. ∘ Performance reduction, loss of financial assets, endangering of service level agreement and security commitments. ∘ Adversarial data inputs can be injected automatically and repeatedly resulting in DoS and resource exhaustion.	∘ Lack of availability of high quality dataset. ∘ Lack of interpretability to establish accurate cause and effect relationship between data and decision. ∘ Longer training time to generate accurate results. ∘ Higher demand of energy, higher latency, memory and energy resource usages.	∘ Automated collection of immutable dataset from trusted distributed resources. ∘ Use of blockchain based framework. ∘ Reduction in the number of operations used in ML model. ∘ Incorporation of transfer learning.
Security	∘ Possibilities of Open API security threats. ∘ Possibilities of parameter attacks. ∘ Possibilities of identity attacks. ∘ Possibilities of man in the middle attacks. ∘ Possibilities of distributed DoS attacks.	∘ Ensure access provided to authentic envisaged consumers. ∘ "Authentication of entities accessing and manipulating information through intent based interface". ∘ Vulnerability of ML algorithms. ∘ Prevention mechanisms for impersonation of SDN applications, controllers and switches. ∘ Policy-driven automation through security issues.	∘ Perform authorization using technologies like OAuth2.0 and JWT tokens. ∘ Use of RBAC, ABAC and Access Control Lists for limiting access to APIs and related operations. ∘ Use of GANs to prevent adversarial attacks. ∘ "Dynamic policies to be defined for network functions and services". ∘ Creation and activation of specific policy definitions for each section of the deployment.
SDO and Projects	∘ Use cases and requirements related to E2E automation. ∘ Areas of automation include SLA management, multi-domain orchestration, infrastructure resource management, data analytic, policies and constraints, and network maintenance. ∘ NS management is supported through the automation of E2E network.	∘ "Need for coordination between SDOs, open source projects and the relevant project initiatives". ∘ Need for coordination between coordination with the verticals and Industry 4.0. ∘ Need to define and study the 5G E2E zero touch network and service management.	∘ Provide clarity on key use cases and their relevant requirements in the organization. ∘ Automation of automation of E2E network service management. ∘ Structured service management to be deployed across multiple technologies or domains in various organizations namely NFV, MEF, OSM and BBF.
Other Technical	∘ Limited AI. ∘ Scalability. ∘ Ethics. ∘ Privacy. ∘ Skill Issues.	∘ "Helps to implement cognitive processing to ZSM system but has but have performance and legal issues, availability of dataset, lack of interpretability of AI/ML model". ∘ Achieve scalability in the ZSM network Conduct activities ethically in the ZSM network. ∘ "Need is to achieve faster service activation in reduced operational cost, ensuring better scalability and lesser human errors". ∘ Limitations of skilled labour having significant impact on operational practices.	∘ Collaboration and data sharing between mobile operators to improve accuracy and inference time, automated collection of trusted immutable datasets, automatic generation of interpretations. ∘ Generate algorithms to perform tasks related to RRM functionalities in 5G RANs. ∘ Generate frameworks to ensure AI is developed and operated with interpretability. ∘ Deployment of automation, additional security tools to achieve optimum level of security. ∘ Use of intent modeling and simulation which can be implemented through an intent model.

7.2. Automation

7.2.1. Lessons Learned and Open Issues

It is necessary to have a framework when translating the business goals into effective management of autonomic functions (AFs). The challenges in automation are identified in five different functional spectrums relevant to business language, translations, policy, reasoning, and configuration enforcement. There exist specific issues when multiple AFs are compared with each other. The intent-based approach is used as a predominant means of automation. In an intent-based approach, the intelligent system or software understands the user goals and converts them to network configurations. The traditional automation techniques fail to perform to their level best form in heterogeneity and situations lagging adaptability. Autonomous systems rely on closed controlled loop structures to fulfill their essential operation. Some of the most common closed control loops exist in MAPE-K, MRACL, and OODA. The distinct functions and systems have the potential to comprehend closed-looped operations. In the case of such systems, the functions are chained to achieve the closed-loop process. Thus, it becomes highly significant to understand the system's functional level of design and its external functional characteristics defining the respective autonomous behavior. The basic objective is to develop pre-defined rules capable of triggering programmed spontaneous actions to initiate an exceptional event. The possible situations that would trigger an automatic reaction are timing of the day, load threshold level, failure, or combination of all the factors. The major open issues include Complexity of the networks and services as a result of increased development in network technologies, the network layers, and its dynamics. There is also need for a business language in case of network governance that enables an operator to articulate the necessities of the network. The concept of reasoning can also be exploited in network governance when mediating between separate domains. There exists dire requirement for policies that aim to select an optimal configuration of services to further disseminate the same from the business level to lower-level hierarchy. [49].

7.2.2. Possible Solutions

There exists a dire need to decrease the overall complexity of the network resulting from transformation of the network into programmable, software-based, service-oriented, and intricately managed architectures. Also, there is a necessity to achieve the accelerated operational capability to support newer business opportunities based on NS. The possible solutions include using specific business rules and solutions when initiating efforts to map higher-level goals with the relevant network resources to deliver a human-friendly governance interface. Appropriate guidance for infrastructure behaviors could be provided during the process of service view. Also, the operator needs to be helped to express goals, objectives, constraints, and rules for smooth functioning of the autonomic network [49].

7.3. E2E LC Management

7.3.1. Lessons Learned and Open Issues

The E2E intelligent services of the ZSM network run the closed loops to manage the benefits of its domain. It includes precise service-oriented predictions based on service demands, demand analysis, and its execution process, ensuring optimization of the E2E service. The demand analysis and resultant decisions taken are based entirely on the data collection and standard data services. Hence there exists possibilities of data manipulation, leading to erroneous results being generated from the ML model. This also leads to deterioration in the performance, loss of financial assets, endangering of service level agreement and security commitments. There are chances that an attacker may create manipulated data samples and feed them into the ML model in an E2E service intelligent system. The generated results would include erroneous predictions on E2E service requirements and also policies to manage the same. The domain intelligence services are also prone to similar types of attacks. The ML model in domain intelligence services generates scale-in or scale-out decisions in a VNF auto-scaling scenario. If the metric data fed into the ML model is authentic, the ML model will generate scale-in choices to reduce costs. On the contrary, if the data is crafted, the ML model would generate scale-out decisions, leading to new VNF instances. To make it worse, adversarial data inputs could be injected automatically and repeatedly, resulting in DoS and resource exhaustion [37]. Some of the predominant open issues include lack of availability of high-quality dataset to

be fed into the ML model in an E2E service management systems. There is also lack of interpretability for developing precise cause and effect relationship which connects the input data with the resultant decisions. As a result it takes longer training time to generate accurate results to complex problems pertinent to E2E service management. Lastly, the higher demand of energy, higher latency, memory, and energy resource usages also act as a plausible issue.

7.3.2. Possible Solutions

The most appropriate solution would be the use of the automated collection of immutable datasets from trusted distributed resources. Also, blockchain-based frameworks would help avoid data manipulation, thereby ensuring the integrity of the dataset. There is also the need to design interpretation approaches to improve the working of the ZSM black box ML models without compromising the accuracy. The number of operations could be reduced in the ML model to optimize using hardware-based methods. Transfer learning techniques could be incorporated so that the experience gained from one AI/ML model could predict data patterns in other models. For example, the DoS attack prediction experience in one E2E service management system could be used to detect DoS in another E2E system [37].

7.4. Security

7.4.1. Lessons Learned and Open Issues

There exist various forms of security threats emerging from technologies used in a ZSM system which are discussed below:

Open API security threats: APIs refer to technologies that integrate various applications with web technology. They help to communicate and interact between the components in the ZSM framework. These APIs play a significant role in the management and coordination of services in the ZSM structure. But they are prone to attacks that intend to get unauthorized access and control of the ZSM databases. These attackers could be compromised senior management personnel, E2E service head, or any customer. These attacks result in data loss, data leak, data unavailability, identity threats, system breaches, and compromises. Some of the widespread API security attacks are parameter attacks, Man in the Middle attacks, identity attacks, and (Distributed) DoS attacks. Parameter attacks manipulate the data fed into an API, including the query parameters, URL, and HTTP header post content. Identity attacks create manipulated data that is used for authentication, authorization, and tracking of the sessions. In a man-in-the-middle attack, the attacker exists between the API provider and the service provider. The attacker accesses the API messages and views confidential information leading to highly critical security breach incidents. In the case of DoS, the API gets loaded with massive information making it non-responsive [35]. The open issues include the need to assess the vulnerability of the ML algorithms in the ZSM framework. There exists requirement for prevention mechanisms to replicate the SDN applications, controllers, and switches. Policy-driven automation could be implemented which would solve issues pertinent to policy enforcement, resolve security issues relevant to the creation, management and enforcement of policies.

7.4.2. Possible Solutions

The immediate solution would be to perform authorization using technologies like OAuth2.0 and JWT tokens. These tokens provide permission to achieve the least essential requirements. The Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Access Control Lists could be used to ensure fine-grained authentication limiting its access to APIs and related functionalities. The exchange of intents could be conducted through secure transport protocol, namely, TLS 1.2, which ensures intent integrity, thereby preventing sniffing and tampering attacks. The validation of inputs, defensive distillation, adversarial training, and use of Generative Adversarial Networks (GANs) could be implemented to prevent malicious activities compromising the ML model in the ZSM. The dynamic policies could be defined for network functions and services. Moreover, the creation and activation of specific policy definitions for each section of the deployment should be managed appropriately for the seamless functioning of the ZSM framework [35].

7.5. SDO and Projects

7.5.1. Lessons Learned and Open Issues

The technical requirements found in various organizations, namely MEC, NFV, ENI, SA2/SA5, 3GPP, and OpenStack, are related to E2E automation of network service management. The potential areas of automation include multi-domain orchestration, SLA management, infrastructure resource management, data analytic, policies and constraints, network maintenance, management, and orchestration. The architecture framework identified in similar organizations tends to provide various options as management domains in the ZSM network for automated management of the E2E network. The service capabilities or management functionalities specified in the same organizations are used to conduct data collection, service orchestration, and resource control. These are further referred by the specific domains ensuring network service management and E2E service management. The same organizations also support the NS management through the automation of the E2E network to create E2E network slices [57]. There is a need for synchronization between the SDOs, open-source projects within the verticals, Industry 4.0 and beyond to collect the requirements. There exists need to define within the verticals, Industry 4.0 and beyond to collect the requirements.

7.5.2. Possible Solutions/ Future Works

It is essential to mention that the ZSM needs to further identify and check on the critical use cases and their relevant organization requirements. This could also help in automating E2E network service management. The architectural design principles and best practices of 3GPP SA5 could be referred to for extension of ZSM architecture enhancement and extension. Structured service management could be deployed across multiple technologies or domains in various organizations, namely NFV, MEF, OSM, and BBF. It needs to be validated if the E2E management domain could support the activities performed by these organizations for the unified functioning of the E2E network and services. The functions pertinent to integration fabric could be differentiated into management functions and orchestration functions. Lastly, it is required to check if closed-loop automation, intelligence, and analytics could be rendered for automation in the aforementioned organizations [57].

The possible mitigation efforts and best practises that can be adopted to develop a more resilient ZSM system are mentioned below:

- Need to ensure that authentic envisaged consumers are allowed to access and communicate with ZSM's APIs.
- Authentication of entities accessing and manipulating information passed by the intent-based interface.
- Need to assess the vulnerability of the ML algorithms in the ZSM framework
- Prevention mechanism to replicate the SDN applications, controllers, and switches.
- Achievement of policy-driven automation through solving issues pertinent to policy enforcement, security issues in creation, management, and enforcement of policies. Identify ways to map administrative roles with relevant problems and their detection, focusing on conflict resolutions between policies.

7.6. Other Technical Challenges

7.6.1. Limitations related to AI

Technologies like Artificial Intelligence (AI) in association with ML and big data analytics are considered as predominant methodologies aiding the implementation of such completely automated networks. AI and related techniques play a significant role in enabling automated self-managing functionalities of ZSM, ensuring enhanced service delivery with a reduction in operating expenses. But the deployment of AI techniques in a ZSM system includes various limitations and risks. AI and ML techniques help implement cognitive processing to the ZSM system, ensuring complete automation but having performance and legal aspects unfulfilled. The network operators expect enhanced service availability and reliability are leading causing network outages and SLA violations, thereby incurring financial losses. Accountability and transparency

are additional factors that need to be emphasized because General Data Protection Regulation (GDPR) expects complete justification on the process involved in decision making by an automated system.

The primary limitation of an AI/ML-based ZSM system includes the availability of a high-quality dataset. The accuracy of any ML model depends on the data set being used, wherein 5G-specific datasets are considered extremely important in developing efficient ML models in a ZSM system. But there exists unavailability of such dataset, and 5G networks were rolled out lately in 2020 with existing operators having privacy issues making them unreachable. The basic requirements in these systems are accurate, suitable, complete, timely data that would provide relevant insights to optimize optimized decision-making. Also, the dataset needs to be high and labeled to train the algorithm efficiently. Such dataset are expensive, not always available or non-feasible which act as a limitation in a ML-based ZSM network [10]

The successful deployment of a completely automated ZSM model depends on the interpretability of its AI/ML model. The interpretability helps to establish the relationship between decisions and the input responsible for such decisions. An accurate interpretation of the AI/ML model helps achieve reliability, accountability, and transparency, but that appears to be a challenging task without compromising the model accuracy. For example, a linear model's interpretability is a reasonably straightforward process expressed as the weighted sum of its attributes. But the same model fails to capture non-linear patterns in the dataset resulting in a reduction of accuracy. Models like ensemble and DL models yield higher accuracy but are often difficult to explain, which necessitates a proper balance between accuracy and interpretability [60]

The success of a ZSM system depends on the capability to manage real-time operations leading to accurate decision making with low latency. The emerging AI/ML techniques, namely deep learning and ensemble ones, resolve complex problems with great accuracy but requires lengthy training time that affects its practicality of real-time usage. Moreover, in a 5G network environment, data patterns keep changing, which requires AI/ML models to be retrained, which restricts performance lags but extends training time. Hence, the achievement of higher accuracy without an increase in training time remains to be a significant challenge in AI/ML model-based ZSM systems. Also, the enhanced accuracy is achieved through compromises in the usage of computational memory and energy resources. Thus, the AI/ML-based ZSM system's leveraging to ensure almost zero latency and low energy usage remain an important challenge.

Possible Solutions/ Future Works

Collaboration and data sharing among multiple mobile operators are essential to ensure enhanced accuracy and speed in the learning process of the ML models. Trust acts as a cornerstone in the deployment of automated systems developed using AI technologies. There are two scopes of trust while achieving accuracy in AI-based systems. The prediction accuracy and efficiency made by ZSM's intelligence services rely on the data collected from varied resources. The integrity and provenance of the trusted resources act as significant contributors to the successful deployment of AI algorithms. The future direction of work lies in the automated collection of secured immutable datasets fetched from different sources. Blockchain technologies have immense potential to play a significant role in developing technical solutions. The model interpretability is also a considerable concern when deep learning and reinforcement learning techniques are used. However, these techniques yield good results but are black box in nature, failing to explain the process involved in generating the output. Automatic generation of interpretations through the efficient design of ZSM frameworks could improve the working of the black-box model without compromising its accuracy.

7.6.2. Scalability

Automation is one of the essential characteristics of a zero-touch network. Automation helps to configure the different components and alter the state of a deployed service without manual typing of commands or restarting of a server. But there exist challenges about the geographically distributed heterogeneous nature of IP and optical backbone networks. The traditional approaches included writing lengthy methods of procedure (MOP) and use more workforce to accommodate increasing deployment schedule [83].

Possible Solutions/ Future Works

ML techniques have been used to develop general-purpose learning frameworks that would potentially create algorithms performing specialized tasks pertinent to Radio Resource Management (RRM) in 5G

RANs. These frameworks are based on reinforcement learning (RL) techniques that include decoupling the RL agent's acting and learning roles. For example, the architecture framework includes one centralized learner and a set of distributed actors. The learner uses the experiences received from the actors for learning the RRM algorithms, and then the actors run the RRM algorithm provided by this learner to generate experiences continuously. This separation of learning and acting roles ensures stability without compromising on training stability. It also provides fault tolerance and creates scope for transfer learning.

7.6.3. Ethics

ML and AI have been significantly implemented to detect the need for change in the network deployment setups, NS, and configuration. The zero-touch network works as an intelligent, self-organizing network that uses ML, artificial intelligence, and data-oriented decision-making. But there exist ethical concerns relevant to possibilities of data manipulation and falsified data injection in the ML models. The possible solutions in this regard are discussed in the next section [10].

Possible Solutions/ Future Works

There has been a practical implementation of AI in the ZSM framework. However, there are many concerns about the various types of disruptions caused by AI-integrated automated tasks. These tasks required human intelligence and communication skills. AI has enabled unattainable insights and decision-making capability based on many integrated data streams that replicate human behavior. The ethical concern lies in two areas. Firstly, due to the possibility of data getting manipulated and secondly, the challenge associated with providing understandable explanations of how predicted outputs get generated. Hence, there exists a demand for generating frameworks and practices that ensure AI is developed and operated in a trustworthy fashion.

7.6.4. Privacy

The ML-based ZSM network is not resilient to adversarial attacks. The negative ML algorithm aims at preventing adversarial attacks and designs techniques to combat the same. The malicious attacks working against the self-organizing cognitive network need to be avoided, requiring more emphasis and attention. The generation of adversarial attacks has been understood, but the process involved in crafting and introducing the attacks in the network traffic is still unknown [35].

Possible Solutions/ Future Works

Automation of the network operators has always been a primary requirement for the service providers. The basic need is to achieve faster service activation in reduced operational cost, ensuring better scalability and lesser human errors. These requirements have led to the establishment of a zero-touch network. But certain security aspects cannot be ignored. For example, in a traditional system, the field service technician performs and monitors the commissioning and provisioning of all the active devices in a network. The technician also ensures maintaining the integrity of the devices and identification of any anomalies. The zero-touch network systems have inherent security controls, but eliminating the risk-mitigating manual commissioning increases the chances of getting exposed to the attacks. Hence to deploy complete automation, additional security tools could be used to achieve the optimum level of security.

7.6.5. Skill Issues

The zero-touch network automation primarily emphasizes on reduction in operation cost. The zero-touch network provides additional benefits of supporting complex network technologies, reducing errors but has limitations regarding skilled labor practices. The zero-touch network is also very complicated to administer. The other major challenge in the state-based zero-touch automation model is its moving parts which have the plausible existence of failure modes. Therefore, a rule-based approach becomes essential to restore the goal state, requiring skilled professionals, thereby posing real challenges [157].

Possible Solutions/ Future Works

The Zero-touch network has the immense benefit of reducing errors and its ability to support complex technologies wherein limitations of skilled labor have a significant impact on operational practices. However, this makes zero-touch networks extremely difficult to administer. Also, the automated tools are primarily rule-based, wherein events are associated with rules that help perform actions. Hence, if the rules become incorrect, the steps would also be erroneous. Thus, the plausible solution would be the use of intent modeling, which can be implemented through an intent model. The state-based model takes a holistic approach which is hugely easier for users to visualize. Therefore, the simulation would be the best possible approach integrating it with automation tools in zero-touch automation systems.

8. Conclusion

Traditional networks and services management approaches cannot keep up with the rapid deployment of new mobile networking services and support ever-increasing connected devices. Thus, a radical change in network MANO in needed in 5G and beyond networks. The ZSM concept has been proposed to offer full E2E automation of network and service management in 5G and beyond networks. Adaptation of ZSM offers more control and visibility into network resources in 5G and beyond ecosystem. This paper comprehensively discussed requirements for automation and basic ZSM architecture with its components to satisfy these requirements. We discussed the goal of ZSM which is to ensure all the network to be executed and managed automatically. In this regard, overview different means of automation, including policy-driven automation, intent-based networking, intent-based service orchestration, network governance, network stability, and use of AI techniques such as transfer learning and deep reinforcement learning are discussed. The paper also summarized ZSM management processes towards the cross-domain E2E service lifecycle such as on boarding process, fulfillment process, assurance process, and optimization. Then, the paper discussed the security issues in E2E service management service, data collection, service analytics, service intelligence, service orchestration, policy management, and closed-loop automation. Finally, the various challenges such as limited AI, scalability, ethics, privacy and skill issues are needed to be address in making a full automation of 5G and future 6G wireless systems by using the ZSM concept.

References

[1] V. W. Wong, R. Schober, D. W. K. Ng, L.-C. Wang, Key technologies for 5G wireless systems, Cambridge university press, 2017.

[2] Q.-V. Pham, F. Fang, V. N. Ha, M. J. Piran, M. Le, L. B. Le, W.-J. Hwang, Z. Ding, A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art, IEEE Access 8 (2020) 116974–117017.

[3] I. Alam, K. Sharif, F. Li, Z. Latif, M. Karim, S. Biswas, B. Nour, Y. Wang, A survey of network virtualization techniques for internet of things using SDN and NFV, ACM Computing Surveys (CSUR) 53 (2) (2020) 1–40.

[4] C. De Alwis, A. Kalla, Q.-V. Pham, P. Kumar, K. Dev, W.-J. Hwang, M. Liyanage, Survey on 6G frontiers: Trends, applications, requirements, technologies and future research, IEEE Open Journal of the Communications Society 2 (2021) 836–886.

[5] J. G. Herrera, J. F. Botero, Resource allocation in NFV: A comprehensive survey, IEEE Transactions on Network and Service Management 13 (3) (2016) 518–532.

[6] W. Kellerer, P. Kalmbach, A. Blenk, A. Basta, M. Reisslein, S. Schmid, Adaptable and data-driven softwarized networks: Review, opportunities, and challenges, Proceedings of the IEEE 107 (4) (2019) 711–731.

[7] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, H. Flinck, Network slicing and softwarization: A survey on principles, enabling technologies, and solutions, IEEE Communications Surveys & Tutorials 20 (3) (2018) 2429–2453.

[8] Q.-V. Pham, M. Zeng, T. Huynh-The, Z. Han, W.-J. Hwang, Aerial access networks for federated learning: Applications and challenges, IEEE Network.

[9] N.-N. Dao, Q.-V. Pham, N. H. Tu, T. T. Thanh, V. N. Q. Bao, D. S. Lakew, S. Cho, Survey on aerial radio access networks: Toward a comprehensive 6G access infrastructure, IEEE Communications Surveys and Tutorials Computing 23 (2) (2021) 1193–1225.

[10] C. Benzaid, T. Taleb, AI-driven zero touch network and service management in 5G and beyond: Challenges and research directions, IEEE Network 34 (2) (2020) 186–194.

[11] M. Bunyakitanon, X. Vasilakos, R. Nejabati, D. Simeonidou, End-to-end performance-based autonomous VNF placement with adopted reinforcement learning, IEEE Transactions on Cognitive Communications and Networking 6 (2) (2020) 534–547.

[12] D. Bega, M. Gramaglia, M. Fiore, A. Banchs, X. Costa-Perez, AZTEC: Anticipatory capacity allocation for zero-touch network slicing, in: IEEE INFOCOM 2020-IEEE Conference on Computer Communications, IEEE, 2020, pp. 794–803.
[13] "Zero-touch network and Service Management (ZSM); Requirements based on documented scenarios", [Accessed on 29.03.2021].
URL https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/001/01.01.01_60/gs_ZSM001v010101p.pdf
[14] "Zero-touch network and Service Management (ZSM); Reference Architecture", [Accessed on 29.03.2021].
URL https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf
[15] "Zero-touch network and Service Management (ZSM); End to end management and orchestration of network slicing", [Accessed on 29.03.2021].
URL https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=54284
[16] "Zero-touch network and Service Management (ZSM); Landscape ", [Accessed on 29.03.2021].
URL https://www.etsi.org/deliver/etsi_gr/ZSM/001_099/004/01.01.01_60/gr_ZSM004v010101p.pdf
[17] "Zero-touch network and Service Management (ZSM); Means of Automation ", [Accessed on 29.03.2021].
URL https://www.etsi.org/deliver/etsi_gr/ZSM/001_099/005/01.01.01_60/gr_ZSM005v010101p.pdf
[18] "Zero touch network and Service Management (ZSM); Proof of Concept Framework", [Accessed on 29.03.2021].
URL https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/006/01.01.01_60/gs_ZSM006v010101p.pdf
[19] "Zero-touch network and Service Management (ZSM); Terminology for concepts in ZSM", [Accessed on 29.03.2021].
URL https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/007/01.01.01_60/gs_ZSM007v010101p.pdf
[20] "Zero-touch network and Service Management (ZSM); Cross-domain E2E service lifecycle management", [Accessed on 29.03.2021].
URL https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=56825
[21] "Zero-Touch Network and Service Managment (ZSM) Closed-loop automation: Solutions for automation of E2E service and network management use cases", [Accessed on 29.03.2021].
URL https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58055
[22] "Zero-touch network and Service Management (ZSM); General Security Aspects", [Accessed on 29.03.2021].
URL https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58436
[23] K. Dev, R. K. Poluru, L. Kumar, P. K. R. Maddikunta, S. A. Khowaja, Optimal radius for enhanced lifetime in IoT using hybridization of rider and grey wolf optimization, IEEE Transactions on Green Communications and Networking.
[24] P. K. R. Maddikunta, T. R. Gadekallu, R. Kaluri, G. Srivastava, R. M. Parizi, M. S. Khan, Green communication in IoT networks using a hybrid optimization algorithm, Computer Communications 159 (2020) 97–107.
[25] A. Osseiran, F. Boccardi, V. Braun, K. Kusume, P. Marsch, M. Maternia, O. Queseth, M. Schellmann, H. Schotten, H. Taoka, et al., Scenarios for 5G mobile and wireless communications: the vision of the METIS project, IEEE communications magazine 52 (5) (2014) 26–35.
[26] X. Foukas, G. Patounas, A. Elmokashfi, M. K. Marina, Network slicing in 5G: Survey and challenges, IEEE Communications Magazine 55 (5) (2017) 94–100.
[27] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, P. Fan, 6G wireless networks: Vision, requirements, architecture, and key technologies, IEEE Vehicular Technology Magazine 14 (3) (2019) 28–41.
[28] T. Huang, W. Yang, J. Wu, J. Ma, X. Zhang, D. Zhang, A survey on green 6G network: Architecture and technologies, IEEE Access 7 (2019) 175758–175768.
[29] B. Holfeld, D. Wieruch, T. Wirth, L. Thiele, S. A. Ashraf, J. Huschke, I. Aktas, J. Ansari, Wireless communication for factory automation: An opportunity for LTE and 5G systems, IEEE Communications Magazine 54 (6) (2016) 36–43.
[30] "Zero-touch network and Service Management (ZSM); end-to-end architectural framework for network and service automation", [Accessed on 29.03.2021].
URL https://www.etsi.org/committee?id=1673
[31] S. Moazzeni, P. Jaisudthi, A. Bravalheri, N. Uniyal, X. Vasilakos, R. Nejabati, D. Simeonidou, A novel autonomous profiling method for the next generation NFV orchestrators, IEEE Transactions on Network and Service Management 18 (1) (2021) 642–655. doi:10.1109/TNSM.2020.3044707.
[32] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, S. Uhlig, Software-defined networking: A comprehensive survey, Proceedings of the IEEE 103 (1) (2015) 14–76.
[33] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, R. Boutaba, Network function virtualization: State-of-the-art and research challenges, IEEE Communications surveys & tutorials 18 (1) (2016) 236–262.
[34] J. Gallego-Madrid, R. Sanchez-Iborra, P. M. Ruiz, A. F. Skarmeta, Machine learning-based zero-touch network and service management: A survey, Digital Communications and Networks.
[35] C. Benzaid, T. Taleb, ZSM security: Threat surface and best practices, IEEE Network 34 (3) (2020) 124–133.
[36] D. Bega, M. Gramaglia, A. Garcia-Saavedra, M. Fiore, A. Banchs, X. Costa-Perez, Network slicing meets artificial intelligence: an AI-based framework for slice management, IEEE Communications Magazine 58 (6) (2020) 32–38.
[37] I. Sanchez-Navarro, P. Salva-Garcia, Q. Wang, J. M. A. Calero, New immersive interface for zero-touch management in 5G networks, in: 2020 IEEE 3rd 5G World Forum (5GWF), IEEE, 2020, pp. 145–150.
[38] A. Oi, R. Sato, Y. Suto, K. Sakata, M. Nakajima, T. Furukawa, A study on automation of network maintenance in telecom carriers for zero-touch operations, in: 2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS), IEEE, 2020, pp. 1–6.
[39] F. Rezazadeh, H. Chergui, L. Alonso, C. Verikoukis, Continuous multi-objective zero-touch network slicing via twin delayed DDPG and OpenAI Gym, in: GLOBECOM 2020-2020 IEEE Global Communications Conference, IEEE, 2020, pp. 1–6.
[40] V. Räisänen, A framework for capability provisioning in B5G, in: 2020 2nd 6G wireless summit (6G SUMMIT), IEEE,

2020, pp. 1–4.
[41] F. Wilhelmi, S. Barrachina-Muñoz, B. Bellalta, C. Cano, A. Jonsson, V. Ram, A flexible machine-learning-aware architecture for future wlans, IEEE Communications Magazine 58 (3) (2020) 25–31.
[42] A. M. Zarca, M. Bagaa, J. B. Bernabe, T. Taleb, A. F. Skarmeta, Semantic-aware security orchestration in SDN/NFV-enabled IoT systems, Sensors 20 (13) (2020) 3622.
[43] V. Ziegler, S. Yrjola, 6G indicators of value and performance, in: 2020 2nd 6G wireless summit (6G SUMMIT), IEEE, 2020, pp. 1–5.
[44] J. Prados-Garzon, T. Taleb, Asynchronous time-sensitive networking for 5G backhauling, IEEE Network 35 (2) (2021) 144–151.
[45] C. Benzaid, T. Taleb, M. Z. Farooqi, Trust in 5G and beyond networks, IEEE Network.
[46] M. Bagaa, T. Taleb, J. B. Bernabe, A. Skarmeta, QoS and resource-aware security orchestration and life cycle management, IEEE Transactions on Mobile Computing.
[47] I. Vaishnavi, L. Ciavaglia, Challenges towards automation of live telco network management: Closed control loops, in: 2020 16th International Conference on Network and Service Management (CNSM), IEEE, 2020, pp. 1–5.
[48] H. Hantouti, N. Benamar, T. Taleb, Service function chaining in 5G & beyond networks: Challenges and open research issues, IEEE Network 34 (4) (2020) 320–327.
[49] R. Rokui, H. Yu, L. Deng, D. Allabaugh, M. Hemmati, C. Janz, A standards-based, model-driven solution for 5G transport slice automation and assurance, in: 2020 6th IEEE Conference on Network Softwarization (NetSoft), IEEE, 2020, pp. 106–113.
[50] I. Afolabi, M. Bagaa, W. Boumezer, T. Taleb, Toward a real deployment of network services orchestration and configuration convergence framework for 5G network slices, IEEE Network.
[51] E. G. ZSM, Zero touch network and service management (ZSM) landscape, version 1.1. 1, ETSI: Sophia Antipolis, France.
[52] Q. Duan, Intelligent and autonomous management in cloud-native future networksâ€"a survey on related standards from an architectural perspective, Future Internet 13 (2) (2021) 42.
[53] A. Boudi, M. Bagaa, P. Pöyhönen, T. Taleb, H. Flinck, AI-based resource management in beyond 5G cloud native environment, IEEE Network 35 (2) (2021) 128–135.
[54] A. Muhammad, T. A. Khan, K. Abbass, W.-C. Song, An end-to-end intelligent network resource allocation in iov: A machine learning approach, in: 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), IEEE, pp. 1–5.
[55] K. Samdanis, T. Taleb, The road beyond 5G: A vision and insight of the key technologies, IEEE Network 34 (2) (2020) 135–141.
[56] J. Baranda, J. Mangues-Bafalluy, E. Zeydan, L. Vettori, R. Martínez, X. Li, A. Garcia-Saavedra, C. Chiasserini, C. Casetti, K. Tomakh, et al., On the integration of AI/ML-based scaling operations in the 5growth platform, in: 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), IEEE, 2020, pp. 105–109.
[57] M. Chahbar, G. Diaz, A. Dandoush, C. Cérin, K. Ghoumid, A comprehensive survey on the E2E 5G network slicing model, IEEE Transactions on Network and Service Management.
[58] O. Hassane, S. Mustafiz, F. Khendek, M. Toeroe, A model traceability framework for network service management, in: Proceedings of the 12th System Analysis and Modelling Conference, 2020, pp. 64–73.
[59] S. Zhang, D. Zhu, Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities, Computer Networks (2020) 107556.
[60] D. Bega, M. Gramaglia, R. Perez, M. Fiore, A. Banchs, X. Costa-Perez, AI-based autonomous control, management, and orchestration in 5G: From standards to algorithms, IEEE Network 34 (6) (2020) 14–20.
[61] M. Xie, J. S. Pujol-Roig, F. Michelinakis, T. Dreibholz, C. Guerrero, A. G. Sanchez, W. Y. Poe, Y. Wang, A. M. Elmokashfi, AI-driven closed-loop service assurance with service exposures, in: 2020 European Conference on Networks and Communications (EuCNC), IEEE, 2020, pp. 265–270.
[62] N. Blefari-Melazzi, S. Bartoletti, L. Chiaraviglio, F. Morselli, E. Baena, G. Bernini, D. Giustiniano, M. Hunukumbure, G. Solmaz, K. Tsagkaris, LOCUS: Localization and analytics on-demand embedded in the 5G ecosystem, in: 2020 European Conference on Networks and Communications (EuCNC), IEEE, 2020, pp. 170–175.
[63] M. McClellan, C. Cervelló-Pastor, S. Sallent, Deep learning at the mobile edge: Opportunities for 5G networks, Applied Sciences 10 (14) (2020) 4735.
[64] Zero-touch network and service management (ZSM); requirements based on documented scenarios (Oct. 2019).
URL https://docplayer.net/193338006-Etsi-gr-zsm-005-v1-1-1.html
[65] B. Moore, E. Ellesson, J. Strassner, A. Westerinen, Policy core information model–version 1 specification, IETF RFC 3060.
[66] A. Westerinen, J. Schnizlein, J. Strassner, M. Scherling, B. Quinn, S. Herzog, A. Huynh, M. Carlson, J. Perry, S. Waldbusser, Terminology for policy-based management, Request for comments 3198.
[67] M. Sloman, Policy driven management for distributed systems, Journal of network and Systems Management 2 (4) (1994) 333–360.
[68] "Intent-based Policy management", [Accessed on 02.10.2021].
URL https://datatracker.ietf.org/meeting/95/materials/slides-95-sdnrg-1.
[69] Z. M. Fadlullah, F. Tang, B. Mao, N. Kato, O. Akashi, T. Inoue, K. Mizutani, State-of-the-art deep learning: Evolving machine intelligence toward tomorrows intelligent network traffic control systems, IEEE Communications Surveys & Tutorials 19 (4) (2017) 2432–2455.
[70] J. A. L. López, J. M. G. Muñoz, J. Morilla, A telco approach to autonomic infrastructure management, in: Advanced Autonomic Networking and Communication, Springer, 2007, pp. 27–42.

[71] A. Martin, J. Egaña, J. Flórez, J. Montalbán, I. G. Olaizola, M. Quartulli, R. Viola, M. Zorrilla, Network resource allocation system for QoE-aware delivery of media services in 5G networks, IEEE Transactions on Broadcasting 64 (2) (2018) 561–574.
[72] I. Alawe, A. Ksentini, Y. Hadjadj-Aoul, P. Bertin, Improving traffic forecasting for 5G core network scalability: A machine learning approach, IEEE Network 32 (6) (2018) 42–49.
[73] "Exposing the Features in IP version Six protocols that can be exploited/extended for the purposes of designing/building Autonomic Networks and Services (2008-2011)", [Accessed on 02.10.2021].
URL https://cordis.europa.eu/project/rcn/85542/factsheet/en.
[74] J. Strassner, N. Agoulmine, E. Lehtihet, Focale: A novel autonomic networking architecture.
[75] N. Koutsouris, K. Tsagkaris, P. Demestichas, Z. Altman, R. Combes, P. Peloso, L. Ciavaglia, L. Mamatas, S. Clayman, A. Galis, Conflict free coordination of son functions in a unified management framework: Demonstration of a proof of concept prototyping platform, in: 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013), IEEE, 2013, pp. 1092–1093.
[76] D. F. P. Rojas, F. Nazmetdinov, A. Mitschele-Thiel, Zero-touch coordination framework for self-organizing functions in 5G, in: 2020 IEEE Wireless Communications and Networking Conference (WCNC), IEEE, 2020, pp. 1–8.
[77] C. H. T. Arteaga, F. Rissoi, O. M. C. Rendon, An adaptive scaling mechanism for managing performance variations in network functions virtualization: A case study in an nfv-based epc, in: 2017 13th International Conference on Network and Service Management (CNSM), IEEE, 2017, pp. 1–7.
[78] L. Ciavaglia, S. Ghamri-Doudane, M. Smirnov, P. Demestichas, V.-A. Stavroulaki, A. Bantouna, B. Sayrac, Unifying management of future networks with trust, Bell Labs Technical Journal 17 (3) (2012) 193–212.
[79] W. Luo, J. Zeng, X. Su, J. Li, L. Xiao, A mathematical model for joint optimization of coverage and capacity in self-organizing network in centralized manner, in: 7th International Conference on Communications and Networking in China, IEEE, 2012, pp. 622–626.
[80] F. D. Calabrese, L. Wang, E. Ghadimi, G. Peters, L. Hanzo, P. Soldati, Learning radio resource management in RANs: Framework, opportunities, and challenges, IEEE Communications Magazine 56 (9) (2018) 138–145.
[81] X. Zhao, L. Xia, J. Tang, D. Yin, " deep reinforcement learning for search, recommendation, and online advertising: a survey" by xiangyu zhao, long xia, jiliang tang, and dawei yin with martin vesely as coordinator, ACM SIGWEB Newsletter (Spring) (2019) 1–15.
[82] M. Jaderberg, W. M. Czarnecki, I. Dunning, L. Marris, G. Lever, A. G. Castaneda, C. Beattie, N. C. Rabinowitz, A. S. Morcos, A. Ruderman, et al., Human-level performance in 3d multiplayer games with population-based reinforcement learning, Science 364 (6443) (2019) 859–865.
[83] F. Rezazadeh, H. Chergui, C. Verikoukis, Zero-touch continuous network slicing control via scalable actor-critic learning, arXiv preprint arXiv:2101.06654.
[84] A. Shaghaghi, A. Zakeri, N. Mokari, M. R. Javan, M. Behdadfar, E. A. Jorswieck, Proactive and aoi-aware failure recovery for stateful NFV-enabled zero-touch 6G networks: Model-free DRL approach, arXiv preprint arXiv:2103.03817.
[85] J. Ali-Tolppa, S. Kocsis, B. Schultz, L. Bodrog, M. Kajo, Self-healing and resilience in future 5G cognitive autonomous networks, in: 2018 ITU Kaleidoscope: Machine Learning for a 5G Future (ITU K), IEEE, 2018, pp. 1–8.
[86] A. Gumbira, Transfer learning in deep convolutional neural networks, Ph.D. thesis, Instytut Informatyki (2018).
[87] S. J. Pan, Q. Yang, A survey on transfer learning, IEEE Transactions on knowledge and data engineering 22 (10) (2009) 1345–1359.
[88] R. Vilalta, P. Alemany, R. Casellas, R. Martínez, C. Parada, J. Bonnet, F. Vicens, R. Muñoz, Zero-touch network slicing through multi-domain transport networks, in: 2018 20th International Conference on Transparent Optical Networks (ICTON), IEEE, 2018, pp. 1–4.
[89] J. P. Fernández-Palacios, J. D. M. Jiménez, V. López, Ó. G. de Dios, D. Larrabeiti, Zero-touch elastic optical networks using sliceable bandwidth variable transponders, in: 2020 22nd International Conference on Transparent Optical Networks (ICTON), IEEE, 2020, pp. 1–5.
[90] I. Boškov, H. Yetgin, M. Vučnik, C. Fortuna, M. Mohorčič, Time-to-provision evaluation of IoT devices using automated zero-touch provisioning, arXiv preprint arXiv:2009.09731.
[91] M. Qin, Q. Yang, N. Cheng, H. Zhou, R. R. Rao, X. Shen, Machine learning aided context-aware self-healing management for ultra dense networks with QoS provisions, IEEE Transactions on Vehicular Technology 67 (12) (2018) 12339–12351.
[92] L. Bonati, S. DOro, L. Bertizzolo, E. Demirors, Z. Guan, S. Basagni, T. Melodia, Cellos: Zero-touch softwarized open cellular networks, Computer Networks 180 (2020) 107380.
[93] J. Fiaidhi, S. Mohammed, Empowering extreme automation via zero-touch operations and GPU parallelization, IT Professional 21 (2) (2019) 27–32.
[94] Selfnet, Selfnet â€“ Framework for Self-Organized Network Management in Virtualized and Software Defined Networks (Feb, 2020).
URL https://selfnet-5g.eu/
[95] CogNet, Building an Intelligent System of Insights and Action for 5G Network Management (Feb, 2020).
URL http://www.cognet.5g-ppp.eu/
[96] SLICENET, End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks (Feb, 2020).
URL https://slicenet.eu/
[97] A. A. Heidari, S. Mirjalili, H. Faris, I. Aljarah, M. Mafarja, H. Chen, Harris hawks optimization: Algorithm and applications, Future generation computer systems 97 (2019) 849–872.
[98] I. Afolabi, J. Prados-Garzon, M. Bagaa, T. Taleb, P. Ameigeiras, Dynamic resource provisioning of a scalable E2E

network slicing orchestration system, IEEE Transactions on Mobile Computing 19 (11) (2019) 2594–2608.
[99] M. Xie, P. H. Gomes, J. Harmatos, J. Ordonez-Lucena, Collaborated closed loops for autonomous end-to-end service management in 5G, in: 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks NFV-SDN, IEEE, 2020, pp. 64–70.
[100] A. Rafiq, A. Mehmood, T. Ahmed Khan, K. Abbas, M. Afaq, S. Wang Cheol, Intent-based end-to-end network service orchestration system for multi-platforms, Sustainability 12 (7) (2020) 2782.
[101] "Zero-touch network and Service Management (ZSM); Cross-domain E2E service lifecycle management", [Accessed on 29.03.2021].
URL https://portal.etsi.org/webapp/workProgram/Report_Schedule.asp?WKI_ID=56825
[102] "ZSM Architectural Framework for End-to-End Service and Network Automation", [Accessed on 29.03.2021].
URL https://sdn.ieee.org/newsletter
[103] J. Ordonez-Lucena, C. Tranoris, J. Rodrigues, L. M. Contreras, Cross-domain slice orchestration for advanced vertical trials in a multi-vendor 5G facility, in: 2020 European Conference on Networks and Communications (EuCNC), IEEE, 2020, pp. 40–45.
[104] N. Saraiva, D. Lachos, C. E. Rothenberg, P. H. Gomes, End-to-end network service monitoring for zero-touch networks.
[105] T. A. Khan, K. Abbass, A. Rafique, A. Muhammad, W.-C. Song, Generic intent-based networking platform for E2E network slice orchestration & lifecycle management, in: 2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS), IEEE, 2020, pp. 49–54.
[106] D. C. Le, N. Zincir-Heywood, M. I. Heywood, Analyzing data granularity levels for insider threat detection using machine learning, IEEE Transactions on Network and Service Management 17 (1) (2020) 30–44. doi:10.1109/TNSM.2020.2967721.
[107] J. Chen, X. Lin, Z. Shi, Y. Liu, Link prediction adversarial attack via iterative gradient attack, IEEE Transactions on Computational Social Systems 7 (4) (2020) 1081–1094.
[108] X. Liu, L. Xie, Y. Wang, J. Zou, J. Xiong, Z. Ying, A. V. Vasilakos, Privacy and security issues in deep learning: A survey, IEEE Access 9 (2021) 4566–4593. doi:10.1109/ACCESS.2020.3045078.
[109] Y. Siriwardhana, P. Porambage, M. Liyanage, M. Ylianttila, AI and 6G security: Opportunities and challenges, in: 2021 Joint European Conference on Networks and Communications (EuCNC) and 6G Summit. IEEE, 2021, pp. 1–6.
[110] T. R. Gadekallu, N. Kumar, S. Hakak, S. Bhattacharya, et al., Blockchain based attack detection on machine learning algorithms for IoT based E-health applications, arXiv preprint arXiv:2011.01457.
[111] K. Ren, T. Zheng, Z. Qin, X. Liu, Adversarial attacks and defenses in deep learning, Engineering 6 (3) (2020) 346–360.
[112] Q. Liu, J. Guo, C.-K. Wen, S. Jin, Adversarial attack on DL-based massive MIMO CSI feedback, Journal of Communications and Networks 22 (3) (2020) 230–235.
[113] H. Yan, X. Li, H. Li, J. Li, W. Sun, F. Li, Monitoring-based differential privacy mechanism against query-flooding parameter duplication attack, arXiv preprint arXiv:2011.00418.
[114] H. Zanddizari, J. M. Chang, Generating black-box adversarial examples in sparse domain, arXiv preprint arXiv:2101.09324.
[115] H. Gu, J. Zhang, T. Liu, M. Hu, J. Zhou, T. Wei, M. Chen, DIAVA: a traffic-based framework for detection of sql injection attacks and vulnerability analysis of leaked data, IEEE Transactions on Reliability 69 (1) (2019) 188–202.
[116] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, M. Ylianttila, The roadmap to 6G security and privacy, IEEE Open Journal of the Communications Society.
[117] S. Sihag, A. Tajer, Secure estimation under causative attacks, IEEE Transactions on Information Theory 66 (8) (2020) 5145–5166. doi:10.1109/TIT.2020.2985956.
[118] Y. Li, Z. Chen, H. Wang, K. Sun, S. Jajodia, Understanding account recovery in the wild and its security implications, IEEE Transactions on Dependable and Secure Computing (2020) 1–1doi:10.1109/TDSC.2020.2975789.
[119] Y. Lee, R. Vilalta, R. Casellas, R. Martínez, R. Muñoz, Auto-scaling mechanism in the ICT converged cross stratum orchestration architecture for zero-touch service and network management, in: 2018 20th International Conference on Transparent Optical Networks (ICTON), IEEE, 2018, pp. 1–4.
[120] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, M. Ylianttila, 6G security challenges and potential solutions, in: 2021 Joint European Conference on Networks and Communications (EuCNC) and 6G Summit. IEEE, 2021, pp. 1–6.
[121] S. Maaroufi, S. Pierre, BCOOL: A novel blockchain congestion control architecture using dynamic service function chaining and machine learning for next generation vehicular networks, IEEE Access 9 (2021) 53096–53122. doi:10.1109/ACCESS.2021.3070023.
[122] Y. Sagduyu, Y. Shi, T. Erpek, Adversarial deep learning for over-the-air spectrum poisoning attacks, IEEE Transactions on Mobile Computing.
[123] M. Javaheripi, M. Samragh, B. D. Rouhani, T. Javidi, F. Koushanfar, CuRTAIL: Characterizing and thwarting adversarial deep learning, IEEE Transactions on Dependable and Secure Computing.
[124] K. Doshi, Y. Yilmaz, S. Uludag, Timely detection and mitigation of stealthy DDoS attacks via IoT networks, IEEE Transactions on Dependable and Secure Computing.
[125] M. A. Azad, S. Bag, C. Perera, M. Barhamgi, F. Hao, Authentic caller: Self-enforcing authentication in a next-generation network, IEEE Transactions on Industrial Informatics 16 (5) (2019) 3606–3615.
[126] G. Carrozzo, M. S. Siddiqui, A. Betzler, J. Bonnet, G. M. Perez, A. Ramos, T. Subramanya, AI-driven zero-touch operations, security and trust in multi-operator 5g networks: a conceptual architecture, in: 2020 European Conference on Networks and Communications (EuCNC), IEEE, 2020, pp. 254–258.
[127] J. Ortiz, R. Sanchez-Iborra, J. B. Bernabe, A. Skarmeta, C. Benzaid, T. Taleb, P. Alemany, R. Muñoz, R. Vilalta, C. Gaber, et al., Inspire-5Gplus: Intelligent security and pervasive trust for 5G and beyond networks, in: Proceedings of the 15th International Conference on Availability, Reliability and Security, 2020, pp. 1–10.

[128] D. J. Miller, Z. Xiang, G. Kesidis, Adversarial learning targeting deep neural network classification: A comprehensive review of defenses against attacks, Proceedings of the IEEE 108 (3) (2020) 402–433. doi:10.1109/JPROC.2020.2970615.
[129] J. Sun, H. Xiong, S. Zhang, X. Liu, J. Yuan, R. H. Deng, A secure flexible and tampering-resistant data sharing system for vehicular social networks, IEEE Transactions on Vehicular Technology 69 (11) (2020) 12938–12950. doi:10.1109/TVT.2020.3015916.
[130] Q. Sun, K. Zhang, Y. Shi, Resilient model predictive control of cyberâ€“physical systems under DoS attacks, IEEE Transactions on Industrial Informatics 16 (7) (2020) 4920–4927. doi:10.1109/TII.2019.2963294.
[131] S. J. Yoo, Neural-network-based adaptive resilient dynamic surface control against unknown deception attacks of uncertain nonlinear time-delay cyberphysical systems, IEEE Transactions on Neural Networks and Learning Systems 31 (10) (2020) 4341–4353. doi:10.1109/TNNLS.2019.2955132.
[132] H. Kumar, H. Habibi Gharakheili, C. Russell, V. Sivaraman, Enhancing security management at software-defined exchange points, IEEE Transactions on Network and Service Management 16 (4) (2019) 1479–1492. doi:10.1109/TNSM.2019.2944368.
[133] "5GZORRO (Zero-tOuch secuRity and tRust for ubiquitous cOmputing and connectivity in 5G networks)", [Accessed on 29.03.2021].
URL https://www.5gzorro.eu/
[134] "Intelligent Security Architecture for 5G and Beyond Networks (Inspire-5GPlus)", [Accessed on 29.03.2021].
URL https://www.inspire-5gplus.eu/
[135] "MonB5G (Distributed management of Network Slices in beyond 5G", [Accessed on 29.03.2021].
URL https://www.monb5g.eu/
[136] "5G-VINNI (Verticals Innovation Infrastructure)", [Accessed on 29.03.2021].
URL https://www.5g-vinni.eu/
[137] "Hexa-X (A flagship for B5G/6G vision and intelligent fabric of technology enablers connecting human, physical, and digital worlds)", [Accessed on 29.03.2021].
URL https://hexa-x.eu/
[138] "6G Flagship", [Accessed on 29.03.2021].
URL https://www.oulu.fi/6gflagship/
[139] "OpenStack", [Accessed on 29.03.2021].
URL https://www.openstack.org/
[140] "Open Source MANO (OSM)", [Accessed on 29.03.2021].
URL https://osm.etsi.org/
[141] "Open Network Automation Platform (ONAP)", [Accessed on 29.03.2021].
URL https://www.onap.org/
[142] "Open Platform for NFV (OPNFV)", [Accessed on 29.03.2021].
URL https://www.opnfv.org/
[143] "ESTI Zero touch network & Service Management (ZSM)", [Accessed on 29.03.2021].
URL https://www.etsi.org/technologies/zero-touch-network-service-management
[144] "3GPP TR 23.791 (V16.1.0): "Study of Enablers for Network Automation for 5G (Release 16)"", [Accessed on 29.03.2021].
URL https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3252
[145] "3GPP TR 23.742 (V1.1.0): "Study on Enhancements to the Service-Based Architecture (Release 16)"", [Accessed on 29.03.2021].
URL https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3457
[146] "3GPP TS 28.521 (V15.0.1): "Performance Management (PM) for mobile networks that include virtualized network functions"", [Accessed on 29.03.2021].
URL https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2970
[147] "3GPP TS 28.311: "Policy management for Network Function Virtualization (NFV) based mobile networks"", [Accessed on 29.03.2021].
URL https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3551
[148] "3GPP TR 32.871 (V15.0.0): "Study on policy management for mobile networks based on Network Function Virtualization (NFV) scenarios (Release 15)"", [Accessed on 29.03.2021].
URL https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3278
[149] "3GPP TR 28.812 V17.0.0 "Study on scenarios for Intent driven management services for mobile networks (Release 17)"", [Accessed on 29.03.2021].
URL https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3553
[150] "Recommendation ITU-T Y.3172: "Architectural framework for machine learning in future networks including IMT-2020"", [Accessed on 29.03.2021].
URL https://www.itu.int/rec/T-REC-Y.3172/en
[151] "TM Forum Open Digital Architecture", [Accessed on 29.03.2021].
URL https://www.tmforum.org/oda/
[152] "Central Office Re-architected as a Datacentre (CORD) platform", [Accessed on 29.03.2021].
URL https://opennetworking.org/cord/
[153] "Intent NBI â€“ Definition and Principles", [Accessed on 29.03.2021].
URL https://opennetworking.org/wp-content/uploads/2014/10/TR-523_Intent_Definition_Principles.pdf
[154] "Network Slicing Use Cases Requirements", [Accessed on 29.03.2021].
URL https://www.gsma.com/futurenetworks/wp-content/uploads/2018/03/Network-Slicing-Use-Cases-Requirements-Wrapper.

pdf
[155] "OASIS Open Data Protocol (OData) TC", [Accessed on 29.03.2021].
URL https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=odata
[156] "Topology and Orchestration Specification for Cloud Applications Version 1.0", [Accessed on 29.03.2021].
URL http://docs.oasis-open.org/tosca/TOSCA/v1.0/os/TOSCA-v1.0-os.html
[157] E. Breverman, N. El-Sakkary, T. Hofmeister, S. Ngai, A. Shaikh, V. Vusirikala, Optical zero touch networking-a large operator perspective, in: Optical Fiber Communication Conference, Optical Society of America, 2019, pp. W3G–4.