IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 20, 2021, accepted October 9, 2021, date of publication October 14, 2021, date of current version October 26, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3120143

Security and Trust in the 6G Era

VOLKER ZIEGLER[1], (Senior Member, IEEE), PETER SCHNEIDER[1], HARISH VISWANATHAN[2], (Fellow, IEEE), MICHAEL MONTAG[1], SATISH KANUGOVI[3], (Senior Member, IEEE), AND ALI REZAKI[4]

[1]Nokia Bell Labs, 81541 Munich, Germany
[2]Nokia Bell Labs, Murray Hill, NJ 07974, USA
[3]Nokia Standards, Bengaluru 560045, India
[4]Nokia Standards, 81541 Munich, Germany

Corresponding author: Volker Ziegler (volker.ziegler@nokia-bell-labs.com)

This work was supported by Nokia.

ABSTRACT A comprehensive set of security technology enablers will be critically required for communication systems for the 6G era of the 2030s. Trustworthiness must be assured across IoT, heterogenous cloud and networks, devices, sub-networks, and applications. The 6G threat vector will be defined by 6G architectural disaggregation, open interfaces and an environment with multiple stakeholders. Broadly decomposed into domains of cyber-resilience, privacy and trust and their respective intersection, we explore relevant security technology enablers including automated software creation and automated closed-loop security operation, privacy preserving technologies, hardware and cloud embedded anchors of trust, quantum-safe security, jamming protection and physical layer security as well as distributed ledger technologies. Artificial intelligence and machine learning (AI/ML) as a key technology enabler will be pervasive and of pivotal relevance across the security technology stack and architecture. A novel vision for a trustworthy Secure Telecom Operation Map is developed as part of the automated closed loop operations paradigm.

INDEX TERMS 6G, security, cyber-resilience, privacy, trustworthiness, sub-networks, wireless networks.

I. INTRODUCTION

Communications in the 2030s will be heavily influenced by 6G technology and its architecture, which will hold significant potential and opportunity to expand and augment human potential. The 6G era will be about connecting the physical, digital and biological worlds to provide humans with new experiences by augmenting our intelligence, producing and consuming new and immersive digital worlds and controlling the automatons of the 2030s. Human lifestyle and possibility will be fundamentally transformed [1], [2]. Notwithstanding, a key prerequisite to realizing the full value and benefit of 6G will be research on cyber-resilience, privacy and trust.

Health monitoring is a good example of why security, privacy and trust deserve the utmost attention. As part of the 'augmenting our intelligence' category of use cases, humans will learn from and with machines in new ways, sense and analyze the physical world through the network, which will essentially provide a sixth sense, i.e., a continuous augmented intelligence overlay through various biological and physical sensors, with the network acting as a sensor and thus a source of intelligence. Such scenarios of augmenting our intelligence may hold special promise for healthcare through in-body monitoring and analysis, thereby connecting with the biological world. Security, privacy and trust considerations should shape system design to strictly avoid any compromise of patient control and anonymity. Data and information must be processed without knowledge of the patient identity if, for instance, processing is done on an untrusted platform.

In the category of creating new and immersive digital worlds, the proliferation of video and online sessions during the pandemic have shown an interest in mixed reality telepresence. In the long term, this may expand to holographic immersion. New privacy solutions will be needed to prevent inadvertent and unauthorized sharing of artifacts within shared video streams.

Other use cases in this category include high resolution mapping for remote driving and transport purposes both indoors (e.g., in manufacturing) and outdoors. This kind of mixed reality co-design is likely to take Industry 4.0 to the next level in the 2030s, but it will need holistic security mechanisms. Industrial operations will go beyond the extensive use of IoT devices and mission critical connectivity, to collaboration between mobile robots, drone swarms, and life-critical

The associate editor coordinating the review of this manuscript and approving it for publication was Xueqin Jiang.

connectivity requiring high accuracy positioning, actuation and sensing. Such industrial use case scenarios will require enhanced mechanism for assurance of identity and privacy of the new autonomous machines and devices to protect intellectual property of the companies involved. Distributed data from sensor fusion will require special information security protection in a world of billions of devices, millions of sub-networks and a wide variety of ecosystems. While several recent papers cover 6G vision and technologies [3]–[8], 6G security and privacy aspects have been sparsely covered in publications such as in [9], [10]. Recent categorized surveys of exclusive 6G literature seem to confirm this [11].

The 6G architectural paradigm [2] will include simplification and convergence of radio access and core networks building on a micro-services and cloud-native approach. The associated change in security paradigm will increasingly be part of 5G deployment evolution beyond what is explicitly specified in the 3rd Generation Partnership Project (3GPP) specification [12] by taking advantage of the information technology (IT) family of technologies [13], [14] as will be described more in Section II; likewise, open source technologies will contribute to security and privacy solutions [15] as a foundation for the 6G era.

While options of redundancy should not be confused with security mechanisms, multi-path routing and enhanced path reliability for software-defined networks (SDN) can also be considered to be part of the end-to-end 5G evolving security architecture. Proliferation of open interfaces in conjunction with co-create vehicles of shared development such as ORAN [16] will help drive the security requirement set in new ways. Future evolution of edge cloud and virtual Radio Access Networks (vRAN) will drive the transformation of massive scale access, while dedicated hardware accelerators will help optimize extreme attributes of 6G performance. 6G hardware and cloud-embedded anchors of trust will contribute to next-generation trustworthiness in terms of the Trusted Execution Environment (TEE) and flexible anchors of trust to ensure system integrity.

To analyze potential 6G security innovation, we find it helpful to associate technology enablers with cyber-resilience, privacy and trust as primary domains of impact. In each of these categories, we discuss new technology enablers that will likely play a role in the 6G security design. AI/ML will be of critical importance to identify novel attacks, although they will also likely be used to create ever more sophisticated attacks in the years to come. We foresee a future where AI/ML will assure security across technologies and the full lifecycle of network development, distribution and deployment.

Trustworthiness in the 6G era will require automated software (SW) creation and automated closed-loop security operations including a vision for a comprehensive Secure Telecom Operation Map (SecTOM).

Privacy preserving technologies such as homomorphic encryption and federated learning will be crucial for various use case scenarios as described above and will complement technology enablers such as hardware (HW) and cloud-embedded anchors of trust. Quantum safe security enablers have the potential to redefine cyber-resilience. Jamming protection and physical layer security (PLS) and distributed ledger are some other security technology enablers of relevance for communications in the 2030s.

This paper takes a holistic and visionary view of 6G security including technology enablers from the physical to the application layer, covering aspects related to specifications, development, deployment and operations.

The novel aspects of this paper are that this is a vision building on research and exposure to debates and discussions with customers, partners and SDOs. Moreover, our security vision is anchored in 6G architecture. This is a condensed overview of the most relevant security technology enablers and secure SW creation and operations are explicitly covered. The new and comprehensive concept of Secure Telecom Operations Map (SecTOM) is introduced. New technology enablers are presented such as edge validation for data integrity and advanced jamming protection.

The paper is structured as follows. In Section II the evolution of 5G security paradigm is described. The expanding 6G threat vector and our view of the challenge of 6G era trustworthiness is introduced in Section III. Section IV will dive deeper into the main aspects of 6G security technology enablers clustered into domains of cyber-resilience, privacy and trust and their respective intersection. In section V, we describe the specific research challenges related to the security technology enablers. We conclude with a summary in Section VI.

II. EVOLUTION OF THE 5G SECURITY PARADIGM

In the Introduction, we briefly outlined the context for a comprehensive 6G security vision to assure security, privacy and trust for the next generation of networks. However, 5G security design has already brought about unprecedented flexibility and transformation compared to previous generations of mobile networks. Hence, it is appropriate, as a starting point, to revisit 5G security evolution as defined and driven by both 3GPP [12] and other standards organizations such as ETSI NFV [13].

3GPP Rel 15 has defined a comprehensive security architecture for 5G [17] including a new access-agnostic authentication framework. Enhanced subscription privacy has been defined to defeat the so-called ''IMSI-catching'' that has been a significant threat to subscriber location privacy in previous mobile network generations. User plane integrity protection has been added to complement user plane encryption. Extensible Authentication Protocol (EAP) based ''secondary authentication'' and network slice specific authentication and authorization is covered by the 3GPP security architecture. New architectural approaches like service-based architectures have new security concepts, including, in this case, not only mutual authentication and transport layer security for all communications between network functions, but also an authorization concept that enables control of service usage

in a granular way between network functions. For interconnection security, the somewhat inflexible 3G/4G approach, which relied solely on IPsec tunnels, has been enhanced by a much more flexible security protocol allowing intermediaries within the interconnection network to apply meaningful treatment of signaling messages in a secure way.

Beyond 3GPP specifications, various security mechanisms such as perimeter security and traffic filtering by virtual firewalls, logically or even physically separated security zones, and traffic separation by Virtual Local Area Networks (VLANs) and wide area Virtual Private Networks (VPNs) will continue to be essential means of protection and differentiated security control during the 5G evolution. Holistic and automated security management and orchestration must be complemented by automated, self-adaptive, intelligent security controls across the 5G network and across all the layers of the architectural stack. As 5G network elements and network functions move to the telco cloud, they are transformed from dedicated and specialized, closely coupled HW and SW units to pure software entities, running on standard IT HW providing a virtualized environment as supported by ETSI NFV. Sound and robust implementations of the virtualization layer, including the hypervisor and the overall cloud platform software as well as security aware implementation of the network functions, are essential for a secure deployment. Moreover, mechanisms must be in place to assure integrity and trust for both platform and virtualized network functions.

Table 1 shows items that we foresee will shape the evolution of the 5G security paradigm in the next several years. Crypto algorithms for the radio I/F will evolve by using 256-bit symmetric keys. Special ''light-weight'' crypto algorithms will be introduced that provide high security but, at the same time, minimize the computational effort for low-energy budget devices. Enhancing privacy protection is high on the 5G security evolutionary agenda. An obvious next step is to strictly enforce single use for temporary identifiers in the non-access stratum protocols. Another step is to improve the authentication and key agreement procedure to further reduce the threat of tracking or linkability attacks, where an attacker may be able to verify the presence of a victim device despite the enhancements in subscriber privacy.

Secure multi-party computing protocols will allow the processing of sensitive data, for example, about security incidents in networks in a privacy preserving manner. New options for secure hardware on end devices should allow for more flexibility and diversity as is, for instance, required with non-public networks. As attacks are expected to become more sophisticated and to no longer be launched mainly in the user plane, but also in the control plane, enhanced control plane robustness on external interfaces such as between device and network may be needed.

We expect to see full operationalization of 5G slicing security management and automation in the coming years. We also expect further evolution of self-adaptive and intelligent 5G security controls by means of intelligent security orchestration, automation and response (SOAR) operational loop (protect-detect-respond) with enhanced response; security management and automation will seamlessly be integrated with the overall 5G network Service Management and Orchestration (SMO) solutions.

TABLE 1. Evolution of 5G security paradigm.

	5G evolution
Crypto algorithms for the radio interface	256bit symmetric keys crypto algorithms enhanced for energy efficiency
Privacy preservation	secure multi-party compute, strict single-use for temporary identifiers
Subscriber and device identifiers, credentials	new options for secure hardware on end devices
Enhanced control plane robustness	on external interfaces such as between UE and network
Network slicing and subnetwork security	5G slicing security mgmt. and automation e2e
NFV, SDN and cloud native security	Micro-services monitoring; platform and workload integrity protection at boot and during runtime
Self-adaptive, intelligent security controls	intelligent SOAR operational loop (protect-detect-respond) with enhanced response
Security management and orchestration	security management & automation integrated with overall 5G network O&M solutions

The transition to, and adoption of, the cloud-native network and lifecycle paradigm will continue for reasons of increased simplicity, lower cost and IT flexibility. Comprehensive micro-services monitoring as well as platform and workload integrity protection will be needed at boot and during runtime. Cloud-native technologies empower service providers and vendors to build and operate scalable applications in dynamic cloud environments and as fostered and supported by Cloud Native Compute Foundation (CNCF) [18]. CNCF has started to analyze the complex arena of security issues and challenges in conjunction with the cloud-native paradigm. The transition to ''DevOps'' [19] will assure an agile framework for continuous delivery and integration for large scale digital production environments; the approach of ''shift left'' moves security concern upstream in the application development process and can therefore be viewed as integral part of ''DevSecOps''. In this context it is to be noted that the number of supply chain attacks keeps growing and securing the software supply chain will continue to be a challenge of relevance. In the subsequent section, we explore the expanding 6G threat vector beyond 5G evolutionary scope and the associated challenge of trustworthiness.

III. THREATS AND TRUSTWORTHINESS CHALLENGE

The stage for threats and challenge of trustworthiness in the 6G era is set by the disaggregated het-cloud architecture [2] in conjunction with softwarization and IT-based infrastructure operations as shown in Figure 1. The het-cloud platform is a heterogeneous, distributed cloud environment at different locations with multiple stakeholders. Applications can be run at different sites such as on-premise, edge and core and in conjunction with a variety of different hardware and software stacks. Clouds can be private, public or hybrid.

As is shown in Figure 1, the concept of het-cloud goes beyond the poly-cloud approach of integrating cloud offerings from various web-scale and dedicated cloud providers. It includes the compute, storage and run-time environment of

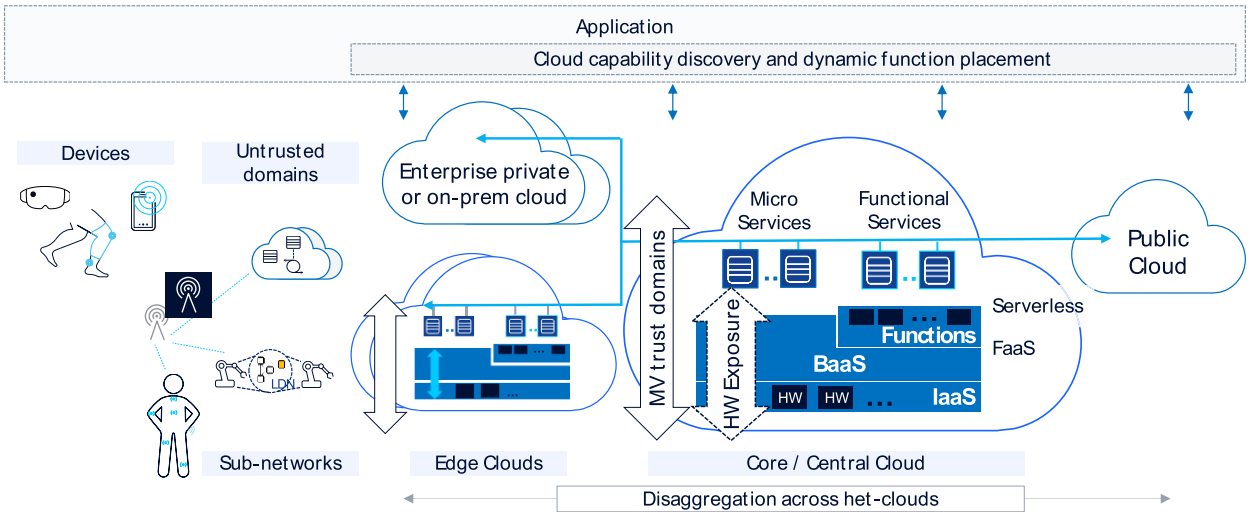

FIGURE 1. Trustworthiness challenge in the age of 6G architectural decomposition [2].

millions of specialized sub-networks, as well as billions of devices and sensors and expands well known challenges of IoT and cloud compute security [20]. This implies a disaggregated architecture with multiple multi-vendor (MV) trust domains across the cloud stack and topology, as well as untrusted domains on a massive scale consisting of sub-networks and devices.

One of the key benefits of the het-cloud architecture is the ease with which new services can be created, placed, subsequently scaled and moved between the clouds, and the efficiency with which they can be executed. Knowledge of the cloud capabilities can be used to optimize service performance, including aspects of security and robustness. Function-as-a-Service (FaaS) as shown in Figure 1 as integral part of the cloud stacks can be considered for selected control plane and management functions to enable enhanced low-start-up delay for execution as well as fast and adaptive locality aware storage access. FaaS will sit on top of Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) stacks, thus making 6G network-related operations and intelligence, as contained in the Backend-as-a-Service (BaaS), of high relevance for security related data collection and analysis, logging and monitoring.

The potential 6G threat vector is illustrated in Figure 2. In the Introduction, we described the context of security and privacy risk exposure for use case families such as augmenting our intelligence, producing and consuming new and immersive digital worlds as well as controlling automatons. Billions of sensors and devices and new human machine interfaces (HMI) will form the basic stratum of threat. On the network side, millions of untrusted specialized sub-networks and their associated dynamic performance attributes will redefine the arena for attacks, including the risk of malicious appropriation of authentication and identity. 6G open interface and disaggregated architectural changes will allow for the possibility of attacks with open service enabling and the monetization of resources in het-cloud domains.

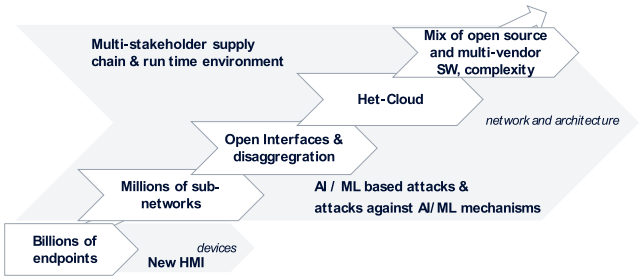

FIGURE 2. Expanding 6G threat vector.

At the same time, the het-cloud paradigm will create new dimensions of risk from multiple stakeholders, such as vendors and operators, as well as multi-stakeholder supply chains with continuous integration and development. The mix of open source and multi-vendor software will create complexity and risk. AI/ML mechanisms will likely not only be a key security technology enabler, but also be used to create more sophisticated threats against the same AI/ML mechanisms within the 6G architecture. From this, it is no surprise that trustworthiness has been identified as a key value objective and indicator for 6G by the European Union 6G flagship project Hexa-X [21].

IV. 6G SECURITY TECHNOLOGY ENABLERS

In our 6G security vision, we cluster security technology enablers into domains of cyber-resilience, privacy and trust, and their respective intersection as shown in Figure 3. Our approach emphasizes the need to extend cyber-resilience technologies such as automated SW creation, automated closed loop security operation, quantum safe cryptography physical layer security and jamming

protection by privacy-preserving technologies and on top of that, trust-creating technologies such as HW and cloud embedded anchors of trust and distributed ledger in order to achieve the ultimate goal of trustworthy 6G networks. We consider resilience against all kinds of cyber-attacks as the core element and indispensable foundation – a network that lacks these attributes of cyber-resilience will not be able to protect privacy and enable trust. While cyber-resilience protects privacy against external attacks, end users may in addition want to reduce the amount of sensitive information that is revealed internally, i.e., to the multiple stakeholders involved in providing the communication services. Here, enabling technologies beyond those in the area of cyber-resilience are needed. By adding specific technologies focusing on creating trust, we complete the overall picture of a resilient, privacy-preserving and trustworthy 6G network. In this paper and as shown in Figure 3, we have decomposed technology enablers into the following categories: pervasive AI/ML, automated SW creation, automated closed loop security operation, privacy preserving technologies, HW and cloud embedded anchors of trust, quantum safe mechanisms, jamming protection and physical layer security as well as distributed ledger.

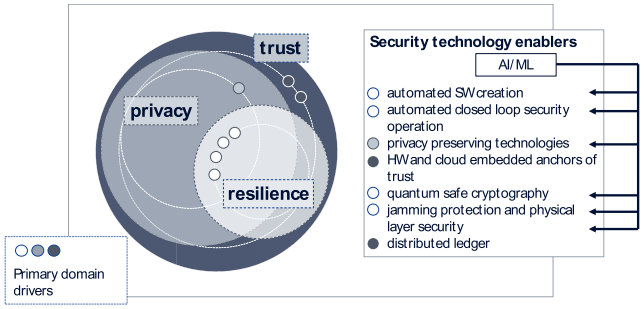

FIGURE 3. 6G security technology enablers as primary drivers of resilience, privacy and trust.

Successful standardization has been the cornerstone of a unified technology landscape that has enabled the proliferation of the mobile communication generations to date. The ecosystem of standardization organizations that have been involved in the architecture and specification of 4G and 5G systems have their sights firmly set on the 6G future as well. Timing is of the essence for creating the optimal impact of standardization. Most SDOs start with studies on technology enablers first before moving into a normative phase of specification. While we expect normative 6G standardization work to start no earlier than 2024/25, we see the precursors of related studies in several technology fields, which we reference in the following.

Pervasive use of AI/ML can be considered a mega-trend of security relevance and driving force to help define the next generation of the Telecom Operation Map (eTOM) [22] and business process framework. In Section B, AI/ML is identified as one of the key drivers for a comprehensive vision of a Secure Telecom Operation Map (SecTOM) for the 6G era. AI/ML will enable and transform automation and analytics for e2e delivery of services to customers as well as for processes to design, create, deliver and support the entire software lifecycle. AI/ML-enabled 6G must include an AI/ML-enabled 6G security architecture in both SW creation and network operations. Notwithstanding, the complexity and the challenge of continuous adaption requires practical implementations of such a concept, without detailed continuous logging and synchronization across the stacks and processes, but rather, based on smart and representative thread sampling. Mitigation of adversarial attacks will need dedicated research as part of a comprehensive "AIOps" paradigm (cf. Section B), which will include adversarial training to improve robustness, continual adaption of the algorithms that an ML model uses to classify data, and omni-present checks for consistency and integrity of the ML models.

In short, AI/ML will be used pervasively across 6G security architecture, process and technology domains. As discussed in Section III, along with its benefits, there will be new and emerging threats rooted in AI/ML. ETSI Industry Specification Group (ISG) Securing Artificial Intelligence (SAI) is already working on these aspects and this domain will gain more significance with the proliferation of AI/ML use towards 6G.

With AI/ML-supported, automated SW creation and secure network operations, 6G will address two of the major root causes of unsatisfactory security in today's information and communication technology systems: vulnerable software and unsecure operational practices. Beyond this, 6G cyber-resilience clearly requires quantum-safe cryptography, considering the progress in the area of quantum computing. Physical layer security, i.e., exploiting the 6G radio technology not only for higher data rates and lower latency, but also for improved security, complements the set of cyber-resilience enablers we consider most relevant for the 6G area. Clearly, on the way towards 6G, these technology enablers will need to be broken down into more granular security mechanisms, and further refined and optimized. To some degree they will also be part of the expected 5G security evolution, as described in Section II. New requirements as coming up in the future as well as yet unknown technologies may also call for enhancing this initial set of cyber-resilience technology enablers.

Building on cyber-resilience, it is commonly agreed that privacy-preserving technologies need to be enhanced in 6G.

In our high-level view, we group all these into a single technology enabler, but we discuss the relevant technologies one-by-one in the following sub-section C. To complete the picture, two technologies aiming at enhancing trust are essential for trustworthy 6G networks: First, HW trust anchors that are resistant against tampering via software, with the challenge to apply them in a highly dynamic cloud environment, where workloads are no longer tightly coupled to specific hardware platforms. Second, distributed ledger technology is an excellent fit for the highly distributed, multi-stakeholder environment that we expect in 6G. Rather than building trust

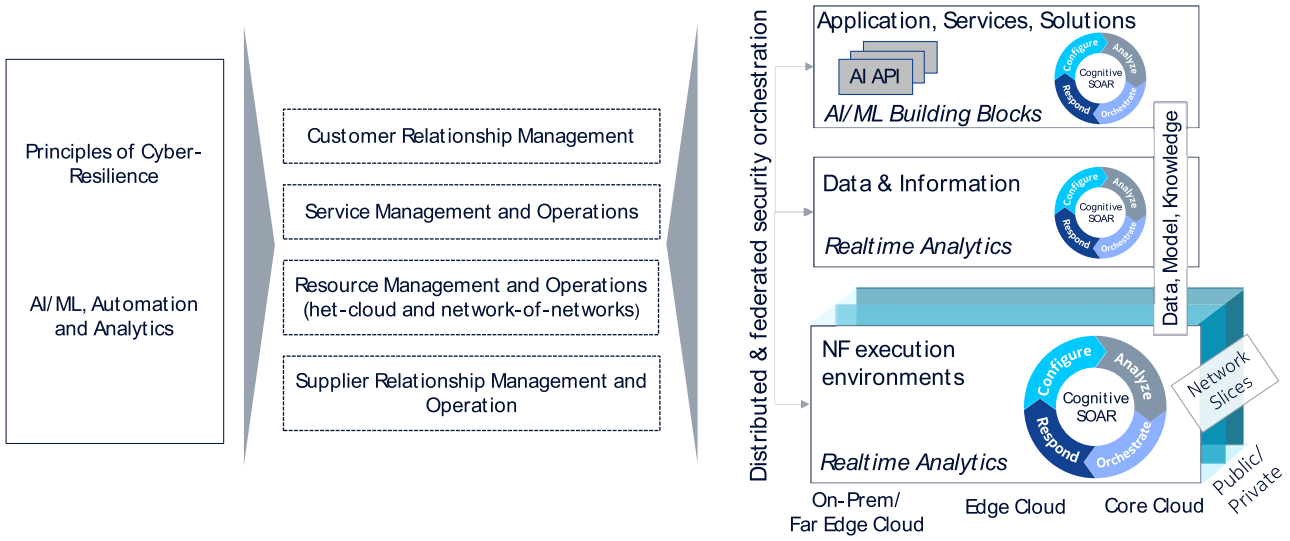

FIGURE 4. Secure telecom operations map for the 6G era.

solely on single, centralized network functions controlled by single stakeholders, DLT allows to base trust on a distributed set of entities controlled by different stakeholders, where no single stakeholder will be able to compromise the common assets.

In the following sub-sections the eight technology enablers for the 6G era as shown in Figure 3 will be analyzed and discussed.

A. AUTOMATED SW CREATION

Many of the security breaches in today's information and communications technology systems are made possible by vulnerable software. While there seems to be a general consensus that there is no such thing as bug-free software, at least under typical economic constraints in terms of cost and time-to-market, AI/ML-enabled, automated SW creation will bring about a shift of paradigm in the 6G era. AI/ML will support software quality and customer-readiness assessment, as well as provide insights on characteristics of code during continuous development and integration.

AI/ML-driven SW creation use cases will include the detection of static and dynamic bugs, code optimization to avoid duplication and deviation from coding guidelines, automated code generation as well as automated testing. As an example, a software versioning and revision control system may use bug reporting information to automatically create code samples labeled with their respective defects. It could then create from these samples a model predicting the likelihood of defects in new software that is submitted to the system, identify the software constructs that are likely to be defective and propose how to correct them.

Together with continuous application performance improvement during each DevOps phase, this can achieve performance and security quality goals that will define the SW creation paradigm of the 2030s. This may include machines writing the code, measures of auto correction, as well as a variety of AI agents for various tasks. SW creation in the 6G era will increasingly adopt concepts of chaos and performance engineering [23] to build confidence in system capability to withstand unforeseen circumstances. Resilience can be proven proactively using techniques such as experimental and potentially destructive fault injection testing. These could include, for example, subjecting the component to a series of what-if scenarios in a virtual or mixed reality system constructed using digital twins of interacting HW and SW elements. Trusted vendor vs. open source in a multi-stakeholder environment will pose interesting opportunities and challenges to define novel ways of applying the 6G-era SW creation approach [24], [25].

B. AUTOMATED SECURITY OPERATIONS

Automated, distributed, cognitive, closed loop security operations and analytics of 6G networks are part of the novel comprehensive vision of SecTOM. This vision builds on a multi-layered view of the framework of key business processes as defined by eTOM. The framework is enhanced to run a secure, efficient, effective, and agile digital enterprise in the 2030s. Figure 4 depicts an overview of SecTOM in its key dimensions. As is shown on the left-hand side and in the middle part of figure 4, principles of cyber-resilience, as well as the applied methodologies of AI/ML, automation and analytics, will shape the security paradigm of SecTOM across process dimensions of customer relationship, service management, resource management and supplier relationship. Key principles of cyber-resilience to drive SecTOM include the minimum needed persistence level of connections, data and resources with the required level of context awareness. Privilege restrictions in network activities and the "least privilege" principle need to be applied consistently. Distributed monitoring and auditing agents will be needed

to help assure cyber resilience in conjunction with redundancy in architecture, segmentation, partitioning or dynamic isolation, as well as integrity checks.

Also shown, on the right hand side of Figure 4, are distributed and federated security orchestration across the management stack by means of nested SOAR closed loops across a horizontally distributed heterogeneous cloud topology and the vertical stack of the network function execution environment, data and information layer, and applications, services and solutions. This is in seamless alignment with the 6G data and information architecture vision [2] with autonomous AI/ML-based decision-making execution units across all layers of abstraction. Latency between the generation of an event and the inference process need to be minimized. At the same time, data and information layers can be leveraged to connect separated units and provide consistent capabilities across endpoints and the het-cloud.

The 6G SecTOM operations and runtime are consistently enabled by AI/ML mechanisms (i.e., they are AIOps-enabled). Shared data and ML will allow for scalable ingestion and analysis of data generated by the operations environment. Concurrent use of multiple data sources, collection models and analytical technologies will become the norm. This will seamlessly come with observability ''beyond monitoring'', i.e., identifying the ''unknown unknowns'' in a holistic and data-centric way and fully integrated with AIOps. Differentiated anomaly detection and omnipresent monitoring across layers with AI/ML tooling is an integral part of such an approach. Defense will typically move to the edge cloud facilitated by additional compute power, as in processing units. Comprehensive signal pattern analysis and monitoring will become feasible in the medium access control (MAC) layer; seamless network and security operations will include the monitoring of microservice-based system call sequences and thread-level interactions with per microservice granularity. CNCF-driven and cloud-native security for het-cloud may include concepts such as evolved pod security policies [15].

C. PRIVACY PRESERVING TECHNOLOGIES

From our analysis of the 6G era threat vector, it is clear that privacy preservation deserves dedicated attention to assure that society realizes the full value of 6G technologies. There are five key privacy technologies of 6G-era relevance: multi-party computation, federated learning, twin synthesis, homomorphic encryption and edge profiling. These foundational technologies will contribute to the trustworthiness of 6G-era networks in terms of confidential computation, data anonymization, secure identities and advanced attestation.

1) MULTI-PARTY COMPUTATION

Multi-party computation will allow multiple parties to collectively perform computation across the het-cloud, sub-networks and devices (see Figure 5) and receive the resulting output without exposing any party's inputs. As is shown in Figure 5, input data can be flexibly processed across the device-cloud-edge-continuum thereby leveraging compute capability across devices, sub-networks, edge clouds and central cloud to derive desired output data.

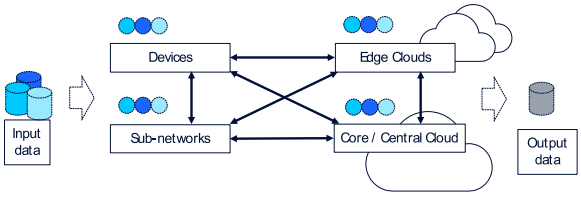

FIGURE 5. 6G multi-party computation across het-cloud, sub-networks and devices.

2) FEDERATED LEARNNG

Federated learning will allow for flexible training of ML models by sending copies of a model to the place where data resides, and for instance, performing training at the edge. Figure 6 depicts an overview of federated learning to assure privacy preservation using decentralized training in a het-cloud-based architecture with cloud capability discovery for resource optimization. Implementing this approach will first require incentive design to motivate the participation of devices and sub-networks in the federated learning model. Novel federated multi-stage learning protocols will be needed, as well as learning model updates, possibly using blockchain.

3) DATA SYNTHESIS

Data synthesis is the systematic and controlled generation of artificial data, which mimics the dependencies and characteristics of a system's real data. Data synthesis is used to extend the data coverage to simplify or just transform a model in cases where no real data, or only spare real data, is available. Methodologies range from simple inter- and extrapolation methods to sophisticated machine learning approaches like Generative Adversarial Networks and Variational Autoencoders.

Synthetic data provides a base for conclusions and outcome from a body of real data evidence. The idea of data synthesis is to carry out the same downstream tasks such as analysis, test-case generation, virtual reality modelling, behavior prediction, and queries on synthetic data, and achieve near-identical results compared to using real data.

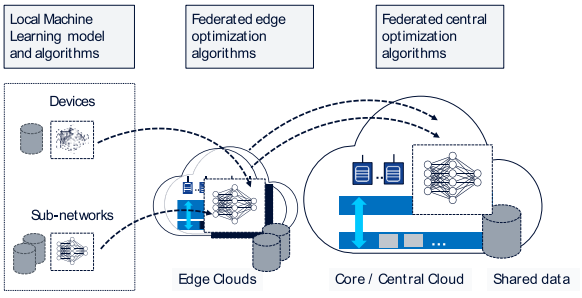

FIGURE 6. Federated learning with multi-stage learning protocols and flexible model updates.

It can be used as a data privacy-preserving technology, when by replacing real data points it also removes privacy sensitive data set features. Privacy can be protected by omitting information from real data set that are not relevant to analysis objectives such as information on owners or the location of users, sensors or sub-networks.

4) HOMOMORPHIC ENCRYPTION

Homomorphic Encryption (HE) allows computation to be directly performed on encrypted data. In the long term, this approach will be valid for all kinds of computations such as for example building a ML model from a huge sample set containing sensitive data. Once decrypted, the result of the computation matches the result from the computation done on clear text data.

5) EDGE VALIDATION FOR DATA INTEGRITY AND PRIVACY ASSURANCE

In the 6G world, with large numbers of human-attached sensors, such as wearables, ear buds, glasses and cameras, there is a significant increase in the risk of privacy loss because of the inadvertent sharing of private information through these sensors. It is highly desirable to have an automated approach to checking and validating the data integrity from these sensors before data are shared with other applications. We envision a network aided solution for such devices in Figure 7.

In the proposed approach, the network restricts transmission of information from specific sensors to only pre-configured data validation applications in the cloud that process the data from the sensors according to preferences set by the user. This is to ensure that the data stream is devoid of private information as needed, i.e., private information that is not sent intentionally or unnecessarily for the purposes of a service. For example, the end user may configure such a data validation application to ensure that no children are present in video streams originating from certain cameras. The application could then monitor any video streams and raise a flag or remove children from the relevant streams. The role of the network is to route traffic from certain end devices to specific pre-configured destinations, namely the validation applications hosted on the edge cloud. The network may identify such traffic through various means, for example, use of special source address ranges, the traffic could be identified as belonging to a specific slice, or some new standardized 'security labels', similar to differentiated service labels, could be added to the packets. Once the data is validated by the application, the data can be either forwarded to the appropriate far-end application or sent back to the user for use with any another application.

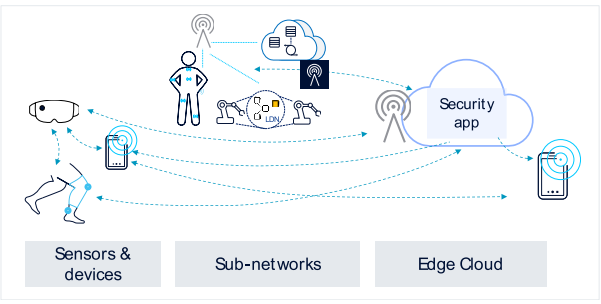

FIGURE 7. 6G sensor data integrity and privacy assurance.

Note that such an approach is relevant in particular when the endpoint itself is not able to clean the data, e.g., due to limited availability of compute power or lack of configurability of such policies at the endpoint. Therefore, this approach may be a powerful way to deliver on objectives of differential privacy, i.e., sharing and processing information related to sensors, devices and sub-networks. The task of data validation can be accomplished by analyzing and describing the properties and patterns within the respective datasets in the edge cloud and withholding information about the individual owners or context such as specific sensor or subnetwork location of the respective datasets.

D. HW AND CLOUD EMBEDDED ANCHORS OF TRUST

The overall 6G trust coverage has to include hardware-based trust anchors and embedded security that are compatible with the het-cloud and HW accelerator-based architectures of the 2030s. In the highly distributed, open and virtualized telecommunications architectures of the future, 6G will also need to use a tamper-resistant secure hardware component, — i.e., root of trust — for its mechanisms to ensure data and code security for deployment over untrusted platforms. Non-public networks and specialized sub-networks are forecast to proliferate in the 6G era and many of them may be operated on-premises or on dedicated cloud stacks, that is, not fully integrated with the wide area network and its mechanisms of trust assurance.

Hardware technologies will include trust anchors and execution environments. They will evolve from today's Trusted Platform Module (TPM) as developed by the Trusted Computing Group (TCG), as well as Secure Boot and Trusted Execution Environments (TEE) and Enclaving [26], [27], which are being leveraged as part of the 5G network evolution. With 6G, we expect advanced options to evolve the TPM and TEE approaches in conjunction with new and hybrid processing units, hardware acceleration and an associated acceleration abstraction layer.

A TPM is usually a tamper-proof secure hardware component isolated from the rest of the processing system and provides secure storage, cryptographic operations (not necessarily acceleration) and a root of trust for reporting. A TEE provides a secure area on a chipset that is used for isolating computations. There are various mechanisms to establish roots of trust out of each of these components, integrating the underlying cloud platforms or abstracting them, respectively, to different degrees. Figure 8 shows an overview of the two concepts and the related context of providing trust coverage and attestation from an anchor of trust all the way to orchestration, application and user levels. A core root of

trust for verification and core root of trust for measurement information, both static and dynamic, can be fed into a TPM; this information is typically utilized in remote attestation and data/key-sealing.

It has been shown that HW assisted TEEs can improve security in a distributed cloud environment and with low performance overhead [28]. The concept of open framework and elastic scaling of TEEs on edge platforms needs to be analyzed more; first studies indicate that privacy and trust can be provided by scalable TEEs for heterogeneous systems (such as a combination of CPUs and GPUs) for performing data intensive computation [29] as needed for demanding 6G use cases such as mixed and augmented reality. Building on the principle of transitive trust [27], TEEs can provide attestation of trust anchored in the confirmed genuineness of enclaves on different processing unit (xPU) levels and of direct relevance to application and user.

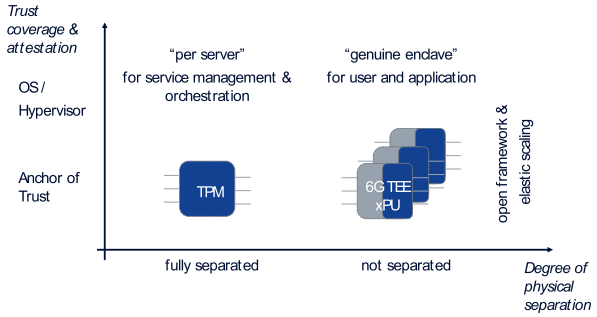

FIGURE 8. 6G anchors of trust, trusted execution environment and trusted platform module.

Attestation is currently on a per-server-basis, but the challenge is extending towards virtual image and container technologies across the het-cloud. The concept of attestation will thus be critical in the orchestration and service management layer as a means to assure supply-chain integrity, data sovereignty and provenance. While the chain of trust starts with one or more trust anchors — i.e., the roots of trust — the objective of maintaining valid trust boundaries along the entire chain will be the result of a combination of platform integrity and embedded anchor of trust technologies as described.

E. QUANTUM SAFE SECURITY

Quantum computing, quantum communications and quantum security mechanisms by means of applied quantum physics are emerging fields of research [30]–[32] with potentially deep implications for security and trust in the 6G era. While the underlying mechanisms of quantum physics in the context of quantum communications are understood, fundamental challenges remain with practical implementations of quantum switches, routers and error correction when building quantum computing infrastructure at scale. However, 6G security should be prepared for a quantum computing future. Implications of quantum computing on the evolution of security will be profound. Asymmetric cryptographic algorithms such as the public-key cryptosystems RSA (Rivest–Shamir–Adleman) and Elliptic-Curve Cryptography (ECC) and security mechanisms like digital signatures or blockchain technology, which depend on them, will be at risk and need to be replaced or extended by quantum-safe variants. Quantum safe cryptography and the security of long-lifecycle data archives need to be actively tackled. While symmetric encryption algorithms such as Advanced Encryption Standard (AES) may be enhanced for quantum safe security by adaptation of parameters such as key size, novel quantum algorithms such as Quantum Key Distribution (QKD) may provide a new approach to secure 6G networks and protocols. Quantum-safe cryptographic algorithms for full cryptographic functionality could provide 6G privacy and trust. Distributed ledgers, such as blockchain, (to be further discussed in Section H) could, for example, be made quantum safe using a two-layer approach. They could use a quantum layer first, with a second layer transmitting messages with tags based on Toeplitz hashing that are using private keys created on the first layer [32]. Quantum safe cryptographic schemes will likely include lattice-based, code-based, multivariate as well as isogeny-based concepts [33]. NIST has identified candidates, splitting them into groups of encryption and signature schemes and describing the hard problems they are trying to solve [34]. 3GPP will likely continue with its efforts to address post-quantum cryptography requirements as already started with studies in conjunction with 5G readiness [35]. Similarly, IETF needs to update and enhance protocol specifications for quantum-safety. Open and aligned integration and standardization across industries and ease of implementation and deployment will be key considerations going forward.

F. JAMMING PROTECTION AND PHYSICAL LAYER SECURITY

1) JAMMING PROTECTION

Jamming has increasingly been identified as a serious threat for vertical markets in conjunction with dedicated and specialized networks. As an integral part of Industry 4.0, availability and cyber-resilience of critical network infrastructure may be seriously impaired by jamming, potentially blocking production and causing economic loss; a simple increase in latency can stop the operation of production lines. Similarly, jamming can pose a serious threat to road safety with connected remote driving potentially becoming a reality in the 6G era. Not to mention 6G use cases of health service provision, where jammers could potentially block the remote monitoring of patients, for instance. Therefore, research into the security design options of 6G physical layer offers the critical opportunity to think of novel ways to mitigate the risk of jamming attacks.

One example approach is shown in Figure 9 depicting, on the right-hand side, a factory hall with various wirelessly connected robots and appliances and under attack from an outside jammer. On the left-hand side of Figure 9, an OFDM resource grid is shown with the two axes of sub-carrier index

and OFDM symbol index and respective data subcarrier, blanked sub-carrier, jammed as well as jammed and blanked subcarrier elements. Blanked resource elements are unknown to the jammer and suitable for detection of jammers. The strategy of mitigation and detection of jamming could include coordinated blanking of physical resource blocks (PRB) and sub-carriers, directional null steering for uplink jamming as well as frequency hopping and spreading. The information about the blank sub-carriers at any given time can be sent privately and securely to the legitimate device for which the PRBs are scheduled as additional scheduling information so that the jammer device does not know the blank locations.

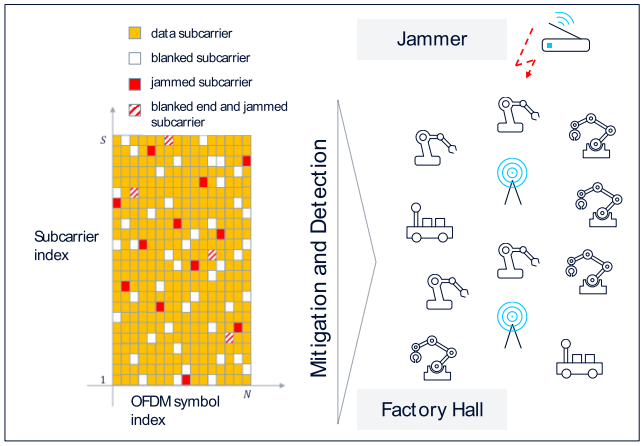

FIGURE 9. 6G security threat from jammimg in industrial environment and mitigating measures.

Notwithstanding, we need to understand the fundamental limits of spectral efficiency for signaling schemes designed to achieve targeted performance of jamming detection and mitigation in order to design the best strategies. Note that besides physical layer methods, cryptographic approaches may be applied as mitigation against smart jamming, i.e., jamming targeting specific, crucial radio resources such as the Random Access Channel (RACH). Specific radio resources for specifically authorized end devices such as public safety devices can be allocated in an unpredictable way. The information about their location in the resource grid can be protected by a frequently changing cryptographic key only known to the authorized devices.

2) PHYSICAL LAYER SECURITY

In the following, we will summarize aspects of physical layer security beyond jamming mitigation, including options for enhanced security that mmW band frequencies may offer.

High-band communications and signaling as enabled by ultra-massive MIMO offer good levels of security due to their high directivity but secrecy capacity is limited by reflections [36], [37]. AI-enabled radio frequency diverse arrays (RFDA) can leverage the superposition of RFDA and artificial noise; with 6G sub-THz bands the associated increase of bandwidth will enlarge the set for randomly allocated frequencies and thus increase the achievable secrecy capacity significantly.

Special schemes in conjunction with cell-free and mesh connectivity 6G architectures [2] may also enhance security anchored in the physical layer. While many of the physical layer security-related schemes face severe challenges in terms of pragmatic implementation, they may hold promise for the billions of devices and sensors which will either be passive or severely energy- and/or compute-power constrained. The dual-use leverage of existing radio communications concepts may be helpful, such as applying physical layer properties at a gateway receiver or sub-network level to authenticate the validity of a transmission [38]. More concretely, two peers communicating via a radio channel may use channel characteristics known and available only to the two peers to achieve origin authentication for messages, without the need to compute and add a cryptographic message authentication code to every message. Channel characteristics may also be used to derive or refresh a shared key between two communications peers.

In this way, PLS methods can complement cryptographic procedures. It should be noted that PLS methods may provide security that is provable by means of information theory, while cryptographic methods rely on the assumption that certain mathematical problems cannot be solved with reasonable effort. Such assumptions on the security of cryptographic methods may no longer hold with the advent of new computing technologies and new algorithms. Quantum computing, for instance, is supposed to break many of the existing crypto-algorithms as discussed in sub-section E above. However, even if a PLS method was provably secure, an implementation of the method is unlikely to be 100% flawless. Eliminating PLS design and implementations flaws that might otherwise allow attackers to break it may turn out to be more difficult compared to implementations of cryptographical methods, where much broader knowledge and experience, both in theory and practice, is available.

Building on the vast amount of literature on PLS and proposals to leverage PLS for node authentication, message integrity, message confidentiality and availability enhancements [39], first papers providing a comprehensive overview and analysis of PLS applicability in 6G have been recently published such as in [40].

G. DISTRIBUTED LEDGER TECHNOLOGIES

Distributed ledger technologies (DLT) such as blockchain are likely to serve as a security and trust enablers for the 6G era [41] in a variety of ways. Being decentralized and multi-stakeholder, they conceptually align with the 6G environment of private and public sensors and devices, sub-networks and het-clouds as shown in Figure 10. Blockchain can be broadly clustered by the nature of the associated consensus rules such as Proof-of-Stake and delegated Proof-of-Stake. Deterministic variants like voting-based consensus algorithms like Byzantine fault tolerant (BFT) are also of relevance [41].

A variety of concepts have been identified to minimize the risk of privacy leakage for DLT [42].

DLT may prove ideal, for example, in securing roaming arrangements. A trend towards specialized and local operators [21] has started to develop in the 5G era, necessitating the need to support various roaming arrangements for service continuity between the local operators and the wide-area operators. The current roaming security architecture relies on prior arrangements for setup and exchange of trust information such as keys and identities, which are used for securing the peer-to-peer roaming links between operators or trusted intermediaries or intermediaries of intermediaries.

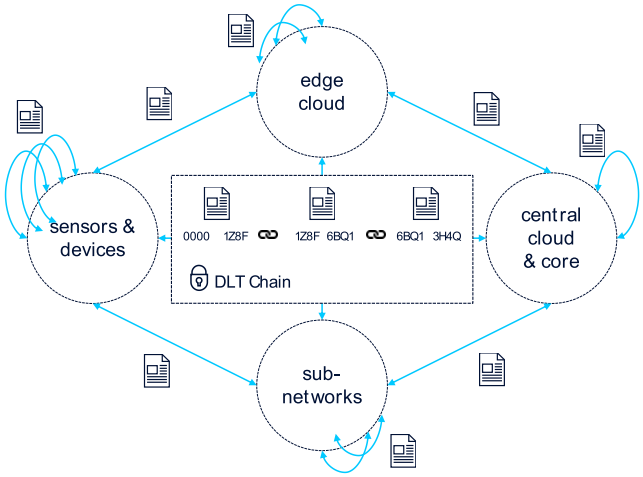

FIGURE 10. Distributed ledger technology chains for trust across sensors, devices, sub-networks and het-cloud.

With increasingly large numbers of distributed network operators and the need to dynamically setup and secure their roaming interfaces, DLT could be used for managing setup of trust across a large number of roaming operators. It offers an ideal fit for storing and exchange of trust information, as well as the use of smart contracts for supporting dynamic roaming policies and contract updates. For example, the distributed ledger (DL) can be used to store the peer's public key, needed for establishing a secure roaming connection between the participating operators. DL procedures enable the key maintenance lifecycle of update, expiration and refresh. In addition, the DL entry for a peer can also include service KPIs, available resources to allow sophisticated roaming peer selection algorithms implemented as smart contracts.

6G will be the era of flexible devices and sensors that can adapt to application needs by leveraging the ubiquitous edge cloud as an extension of its compute, battery and software capabilities. This is an area where DLT can be leveraged to build and share trust information based on observed device behavior [43], which can then be used by the different edge cloud providers to determine the privileges and resources that can be provided to the device. A new device, as part of the registration, can create an entry into the DL. A network manager agent in the serving network can fingerprint and create reports of device behavior deviating from an accepted policy, and store in the DL as records that cannot be tampered with by malicious actors. The DL is then used globally by networks to build device reputation [43]. A network where the device registers for service, may construct a trust level based on historical reports of behavior securely recorded in the DL by the previously served networks, and from this determine the appropriate level of access.

Limitations and challenges of blockchain applicability exist in dimensions of dynamic management and latency as well as scalability as is shown when analyzing blockchain technology for radio access networks in conjunction with concepts such as multi-access-point cooperative transmission and multi-hop data brokerage [44]. Nevertheless, DLT is well suited for a select variety of 6G-related use case scenarios such as trusted roaming and autonomous device management without extreme performance attribute requirements.

V. CHALLENGES OF SECURITY FUTURE RESEARCH

As discussed in the previous section, the security technology enablers have the potential to bring 6G networks to the superior level of trustworthiness that the services of the 2030s will demand. Still, significant challenges of research remain as summarized in this section.

A. AUTOMATED SW CREATION

Vulnerable software is one of the root causes of security issues in today's networks and information technology systems. Towards 6G, as we discuss in section III, the complexity and heterogeneity of the software is expected to rise significantly, increasing the attack surface and thus posing a severe challenge. According to our vision expressed in section IV, application of AI/ML in the software development process has the potential to overcome this threat, by avoiding most, if not all, of the common software vulnerabilities. While research on this is already ongoing, existing approaches are still isolated and immature, and it remains a challenge to fully leverage AI/ML for a highly automated, secure software development.

B. AUTOMATED SECURITY OPERATIONS

The second root cause for security issues, as discussed in section IV, is unsecure network configuration and operation. Again, AI/ML-based automation is the most promising approach to overcome this issue, and the challenge is to advance existing approaches to highly automated, intelligent, self-adapting and holistic orchestration and management systems.

While AI/ML has high potential to boost network security, on the flip side, as discussed in sections III and IV, it also brings new threats. The challenge is on the one hand to secure AI/ML based approaches against targeted attacks, and to make it explainable and trustworthy, and on the other hand to be prepared against potential AI/ML-based attacks. While it is safe to predict that such attacks will happen in the future, their potential extent and impact is currently hard to assess. Close observation of new developments in this area is

a requirement to be able to react timely and keep 6G networks safe.

C. PRIVACY PRESERVING TECHNOLOGIES

AI/ML methods require to collect considerable amounts of data to create precise models, and it may be required to collect such data from various sources across different architectural domains. High precision location and network sensing will create sensitive data in unprecedented quantities. Given this, it is a challenge to ensure confidentiality and privacy of such data not only against external attackers, but also to minimize the amount of sensitive data the various stakeholders need to learn and exchange in order to provide the 6G services.

Considering the huge amount of continuously generated data in 6G networks, a must-have framework of enhanced privacy preserving data processing technologies and inherent principles as discussed in section IV C is needed. The primary objective of such a framework will be how to control and monitor data flows and the data access. New ways of managing and enforcing flexible data security and privacy policies are required by leveraging the distributed 6G het-cloud and edge processing capabilities as well as federated learning concepts. Enhancing data privacy includes challenges and issues of performance to be solved which is particularly true for secure multi-party computation and the promising Homomorphic Encryption technology as well HW- acceleration-based concepts. In addition, a comprehensive theoretical foundation of data privacy models is needed that allows verified model transformations and privacy labeling of data like ''free of privacy sensitive data''. This would particularly support the data synthesis approach and federated learning.

D. HW AND CLOUD EMBEDDED ANCHORS OF TRUST

As pointed out in section IV, hardware-based trust anchors and embedded security are important components of a trustworthy 6G system. While attestation on a per-server-basis works well in today's networks, the challenge in 6G is to extend it towards virtualization and container technologies and make it compatible with the highly flexible and dynamic network deployment in the het-cloud.

E. QUANTUM SAFE SECURITY

In the area of quantum-safe cryptographic schemes, research has already made significant progress, resulting in a number of promising algorithm candidates. It is still required to bring these schemes to full maturity. What must not be underestimated is the effort required to adapt existing security protocols to such new algorithms and achieve consensus on this in an open standardization process.

F. JAMMING PROTECTION AND PHYSICAL LAYER SECURITY

In the area of physical layer security, methods to provide an additional layer of secrecy and integrity should be considered in order to make the 6G radio interface highly secure without compromising 6G KPIs relating to latency, throughput and energy efficiency. PLS mechanisms may even provide provable security properties, different from cryptographic methods that rely on assumptions about the infeasibility of certain computations. As we point out in section IV above, this still leaves the challenge to preserve these theoretical properties in actual implementations that are suitable to support the demanding requirements of the various 6G use cases and are safe even in the presence of sophisticated and resourceful attackers.

The other big challenge in conjunction with the physical layer is protection against jamming. There is an inherent conflict between achieving extraordinary spectral efficiency and making the radio interface highly resilient against jamming. While we have discussed some promising approaches in this paper, we feel the research community is still far from providing a comprehensive set of means against malicious jamming. So, continued and increased research efforts are required to ensure the high degree of availability required by critical 6G services in the presence of jammers.

G. DISTRIBUTED LEDGER TECHNOLOGIES

While the distributed ledger technologies provide a good framework to simplify establishment of trust across heterogenous operator domains and enhance 6G era use cases as well as cumulative trust building based on verified device behavior, a key challenge for practical deployments would be the limits of scalability, energy efficiency and latency of DLT operations. Further work is expected to address the areas of improving scalability of DLT consensus algorithms, making them quantum-safe, while keeping the latency and energy cost under reasonable limits.

VI. CONCLUSION

There is an increasing level of consensus worldwide on the relevance of key indicators of value such as societal acceptance, sustainability and trustworthiness when framing the research agenda for 6G and the 6G era. The ambition is to augment human potential and maximize value for society and humankind with the next generation of networks and to correctly frame and refine the 6G research agenda. From this, security and trust is getting dedicated attention. Government and policy makers will need to be agile in evolving policy in a world of increasingly divergent digital, industrial and operational security standards. Building on current best practice, 6G will depend on suitable standardization and industry collaboration worldwide. The current research vision as we have built through early research and collaborative projects may be adopted by standardization fora in the coming years in the form of studies and subsequent 6G normative specifications. A global agenda of research needs to be developed and refined to assure cyber-resilience, privacy and trust for the future in close alignment with the evolution of 6G, AI/ML, and quantum and cloud technology enablers. Beyond technology enablers, security and automation need to be consistently applied to 6G networks software development

as well as the deployment, operation and management of 6G. The next several years will offer the opportunity to proceed with proof-of-concept and case study work in the domains of key technology enablers as discussed in this paper. Executing on a comprehensive agenda of 6G security research will be a key prerequisite to assure trustworthiness of communications in the 2030.

ACKNOWLEDGMENT

The authors would like to thank a number of colleagues at Nokia Bell Labs with whom they had numerous discussions about security and trust for the 2030s. In particular, they would like to thank P. Baracca, K. Hatonen, I. Oliver, D. Schinianakis, M. Signorini, and J. Urban for their comments on an early draft of this article. They would also like to thank A. Hu for helping with the preparation of the manuscript.

REFERENCES

[1] H. Viswanathan and P. E. Mogensen, "Communications in the 6G era," *IEEE Access*, vol. 8, pp. 57063–57074, 2020, doi: 10.1109/ACCESS.2020.2981745.
[2] V. Ziegler, H. Viswanathan, H. Flinck, M. Hoffmann, V. Räisänen, and K. Hatonen, "6G architecture to connect the worlds," *IEEE Access*, vol. 8, pp. 173508–173520, 2020, doi: 10.1109/ACCESS.2020.3025032.
[3] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, and G. C. Trichopoulos, "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," *IEEE Access*, vol. 7, pp. 78729–78757, 2019.
[4] R. W. Heath, Jr., "Going toward 6G [from the editor]," *IEEE Signal Process. Mag.*, vol. 36, no. 3, pp. 3–4, May 2019.
[5] I. F. Akyildiz, A. Kak, and S. Nie, "6G and beyond: The future of wireless communications systems," *IEEE Access*, vol. 8, pp. 133995–134030, 2020, doi: 10.1109/ACCESS.2020.3010896.
[6] J. Zhang, K. Kang, Y. Huang, M. Shafi, and A. F. Molisch, "Millimeter and THz wave for 5G and beyond," *China Commun.*, vol. 16, no. 2, pp. 3–6, 2019.
[7] T. Nakamura, "5G evolution and 6G," in *Proc. IEEE Symp. VLSI Technol.*, Honolulu, HI, USA, Jun. 2020, pp. 1–5, doi: 10.1109/VLSITechnology18217.2020.9265094.
[8] G. Liu, Y. Huang, N. Li, J. Dong, J. Jin, Q. Wang, and N. Li, "Vision, requirements and network architecture of 6G mobile network beyond 2030," *China Commun.*, vol. 17, no. 9, pp. 92–104, Sep. 2020, doi: 10.23919/JCC.2020.09.008.
[9] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, and O. I. Und. (2020). *6G White Paper: Research Challenges For Trust, Security and Privacy*. Accessed: Mar. 14, 2021. [Online]. Available: http://urn.fi/urn:isbn:9789526226804.
[10] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.
[11] J. R. Bhat and S. A. Alqahtani, "6G ecosystem: Current status and future perspective," *IEEE Access*, vol. 9, pp. 43134–43167, 2021, doi: 10.1109/ACCESS.2021.3054833.
[12] 3GPP. *About 3GPP*. Accessed: Apr. 1, 2021. [Online]. Available: https://www.3gpp.org/about-3gpp/about-3gpp
[13] ETSI. (Oct. 2013). *NFV*. Accessed: Mar. 14, 2021. [Online]. Available: https://portal.etsi.org/nfv/nfv_white_paper2.pdf
[14] L. Peterson, C. Cascone, B. O'Connor, T. Vachuska, and B. Davie, *Software-Defined Networks: A Systems Approach* (Systems Approach Series), 2020. Accessed: Jun. 17, 2021. [Online]. Available: https://sdn.systemsapproach.org and https://github.com/SystemsApproach/SDN
[15] CNCF. (Nov. 2020). *Cloud Native Security White Paper*. Accessed: Mar. 14, 2021. [Online]. Available: https://github.com/cncf/sig-security/blob/efbbd34196882cfd25b691e1b3b50820e9ddd632/security-whitepaper/CNCF_cloud-native-security-whitepaper-Nov2020.pdf
[16] O-RAN. (Feb. 2020). *O-RAN Use Cases and Deployment Scenarios*. Accessed: Mar. 14, 2021. [Online]. Available: https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5e95a0a306c6ab2d1cbca4d3/1586864301196/O-RAN+Use+Cases+and+Deployment+Scenarios+Whitepaper+February+2020.pdf
[17] *Security Architecture and Procedures for 5G System*, document TS 33.501, 3GPP, 2017. [Online]. Available: http://www.3GPP.org
[18] *CNCF*. Accessed: Mar. 14, 2021. [Online]. Available: https://github.com/cncf/foundation/blob/master/charter.md
[19] L. Bass, "The software architect and DevOps," *IEEE Softw.*, vol. 35, no. 1, pp. 8–10, Jan. 2018.
[20] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 964–975, Jan. 2018, doi: 10.1016/j.future.2016.11.031.
[21] *Hexa-X EU, H2020-ICT-2020-2, 6G Vision, Use Cases and Key Societal Values*. Accessed: Mar. 23, 2021. [Online]. Available: https://hexa-x.eu/wp-content/uploads/2021/02/Hexa-X_D1.1.pdf
[22] TMForum. *Business Process Framework (eTOM)*. Accessed: Mar. 23, 2021. [Online]. Available: https://www.tmforum.org/business-process-framework/
[23] A. Basiri, N. Behnam, R. de Rooij, L. Hochstein, L. Kosewski, J. Reynolds, and C. Rosenthal, "Chaos engineering," *IEEE Softw.*, vol. 33, no. 3, pp. 35–41, May 2016, doi: 10.1109/MS.2016.60.
[24] B. Theeten, F. Vandeputte, and T. Van Cutsem, "Import2Vec: Learning embeddings for software libraries," in *Proc. IEEE/ACM 16th Int. Conf. Mining Softw. Repositories (MSR)*, Montreal, QC, Canada, May 2019, pp. 18–28, doi: 10.1109/MSR.2019.00014.
[25] G. Heyman and T. Van Cutsem, "Neural code search revisited: Enhancing code snippet retrieval through natural language intent," 2020, *arXiv:2008.12193*. [Online]. Available: http://arxiv.org/abs/2008.12193
[26] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, Aug. 2015, pp. 57–64, doi: 10.1109/Trustcom.2015.357.
[27] *Hardware-Enabled Security for Server Platforms: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases*, NIST, Gaithersburg, MD, USA, 2020. Accessed: Mar. 14, 2021, doi: 10.6028/NIST.CSWP.04282020-draft.
[28] Z. Ning, J. Liao, F. Zhang, and W. Shi, "Preliminary study of trusted execution environments on heterogeneous edge platforms," in *Proc. IEEE/ACM Symp. Edge Comput. (SEC)*, Seattle, WA, USA, Oct. 2018, pp. 421–426, doi: 10.1109/SEC.2018.00057.
[29] J. Zhu, R. Hou, X. Wang, W. Wang, J. Cao, L. Zhao, F. Yuan, P. Li, Z. Wang, B. Zhao, L. Zhang, and D. Meng, "Enabling privacy-preserving, compute- and data-intensive computing using heterogeneous trusted execution environment," 2019, *arXiv:1904.04782*. [Online]. Available: http://arxiv.org/abs/1904.04782
[30] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future," *IEEE Access*, vol. 7, pp. 46317–46350, 2019, doi: 10.1109/ACCESS.2019.2909490.
[31] D. Schinianakis and E. Martín-López, "Quo vadis qubit?" *Bell Labs Tech. J.*, vol. 23, pp. 1–17, Dec. 2018, doi: 10.15325/BLTJ.2018.2860381.
[32] M. S. Sharbaf, "Quantum cryptography: A new generation of information technology security system," in *Proc. 6th Int. Conf. Inf. Technol., New Generat.*, Las Vegas, NV, USA, 2009, pp. 1644–1648, doi: 10.1109/ITNG.2009.173.
[33] E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. I. Lvovsky, and A. K. Fedorov, "Quantum-secured blockchain," 2017, *arXiv:1705.09258*. [Online]. Available: http://arxiv.org/abs/1705.09258
[34] NIST. (2020). *Post Qunatum Cryptography*. Accessed: Apr. 20, 2021. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography
[35] *Study on the Support of 256-Bit Algorithms for 5G*, document TS 33.841, 3GPP, 2018. [Online]. Available: http://www.3GPP.org
[36] D. Steinmetzer, J. Chen, J. Classen, E. Knightly, and M. Hollick, "Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Florence, Italy, Sep. 2015, pp. 335–343.
[37] Y. Ju, H.-M. Wang, T.-X. Zheng, Q. Yin, and M. H. Lee, "Safeguarding millimeter wave communications against randomly located eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 17, no. 4, pp. 2675–2689, Apr. 2018, doi: 10.1109/TWC.2018.2800747.

[38] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.
[39] M. Shakiba-Herfeh, A. Chorti, and H. V. Poor, "Physical layer security: Authentication, integrity, and confidentiality," in *Physical Layer Security*, K. N. Le, Eds. Cham, Switzerland: Springer, 2021, doi: 10.1007/978-3-030-55366-1_6.
[40] L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, I. Morales, R.-A. Stoica, G. Abreu, and H. Haas, "Physical-layer security in 6G networks," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1901–1914, 2021, doi: 10.1109/OJCOMS.2021.3103735.
[41] T. Nguyen, N. Tran, L. Loven, J. Partala, M.-T. Kechadi, and S. Pirttikangas, "Privacy-aware blockchain innovation for 6G: Challenges and opportunities," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, Levi, Finland, Mar. 2020, pp. 1–5, doi: 10.1109/6GSUMMIT49458.2020.9083832.
[42] H. Lin, S. Garg, J. Hu, G. Kaddoum, M. Peng, and M. S. Hossain, "A blockchain-based secure data aggregation strategy using sixth generation enabled network-in-box for industrial applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 7204–7212, Oct. 2021, doi: 10.1109/TII.2020.3035006.
[43] M. Boussard, S. Papillon, P. Peloso, M. Signorini, and E. Waisbard, "STewARD:SDN and blockchain-based trust evaluation for automated risk management on IoT devices," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Paris, France, Apr. 2019, pp. 841–846, doi: 10.1109/INFCOMW.2019.8845126.
[44] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, "Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm," *IEEE Access*, vol. 7, pp. 9714–9723, 2019, doi: 10.1109/ACCESS.2018.2890557.

VOLKER ZIEGLER (Senior Member, IEEE) received the M.Sc. (Dipl.-Ing.) and Ph.D. (Dr.-Ing.) degrees from the Department of Electrical Engineering, Universität (TH) Karlsruhe, Germany. He has started his career as a Research Scientist with German Aerospace Research/DLR. He has worked as an Information Technology Specialist with World Bank/IFC in the mid-90s. He currently exercises a leadership role in 6G research with Nokia Bell Labs. In his previous role, he was the Head of 5G Leadership and the Chief Architect of Nokia Mobile Networks, he played a key role in defining Nokia e2e 5G offering and positioning Nokia strongly in 5G and associated innovation, technologies, and architecture. Prior to this, he served as the Head of strategy roles for the company and North East region. In more than ten year of his career with Siemens, he has held business unit leadership, finance, sales, services, research and development global roles, and senior positions.

PETER SCHNEIDER received the Diploma degree in mathematics from the Julius-Maximilians-Universität Würzburg, Germany. He started his professional career as a Researcher on new software architectures at the Siemens Corporate Technology Division. He moved on to the Siemens Communication Division, where he investigated and prototyped new, innovative communication solutions, and subsequently became a Systems Engineer at the Siemens Mobile Core Network. Since about 15 years, he has been focusing on network security research at Siemens, Nokia Siemens Networks, and Nokia. In 2015, he joined the Nokia Bell Labs Security Research Group as a Senior Expert for mobile network security. He is the author of various mobile network related security concepts, articles, tutorials, and book chapters, as well as numerous patents and patent applications.

HARISH VISWANATHAN (Fellow, IEEE) received the B.Tech. degree from the Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai, India, and the M.S. and Ph.D. degrees from the School of Electrical Engineering, Cornell University, Ithaca, NY, USA. Since joining Bell Labs in October 1997, he has worked extensively on wireless research, ranging from physical layer to network architecture and protocols, including multiple antenna technology for cellular wireless networks, multi-hop relays, network optimization, network architecture, and the IoT communications. From 2007 to 2015, he was with Corporate CTO Organization, where as a CTO Partner, he advised the Corporate CTO on technology strategy through in-depth analysis of emerging technology and market needs. He is currently the Head of the Radio Systems Research Group, Nokia Bell Labs. He has published extensively more than 100 publications. He is also a Bell Labs Fellow.

MICHAEL MONTAG received the M.Sc. (Dipl.-Inform.) degree in computer science from Universität Hamburg, Germany, in 1990. Then, he joined Siemens Corporate Research working in the area of artificial intelligence, truth maintenance systems, qualitative reasoning, and model-based expert systems for fault diagnosis and configuration. In 1998, he started his career in the area of information and communication data and network security, first still at Siemens. Since 2007 at Nokia Networks Research and currently at Nokia Bell Labs, where he is currently leading the security research teams and managing the security research and innovation portfolio.

SATISH KANUGOVI (Senior Member, IEEE) received the B.E. degree from the Delhi College of Engineering, University of Delhi, India. Currently, he heads the Nokia Standardization and Industry Engagements, APAC Region. He is also a Distinguished Member of Technical Staff (DMTS). In his earlier roles, he has been part of Robotic Systems Research at the Enterprise and Industrial Automation Department, Nokia Bell Labs, and Mobile Networks CTO, focusing on wireless research and standardization. He has around 22 years of experience in e2e solutions architecture, including conceptualization, standardization and productization of innovative ideas into products. He has been involved in wireless standards development as a delegate in 3GPP/3GPP2. He has been the author of multiple RFC/drafts at IETF focusing on the areas of interworking and multi-access. He has authored and coauthored several publications and been granted numerous patent families.

ALI REZAKI received the B.Sc. and M.Sc. degrees from the Department of Electrical and Electronics Engineering, Middle East Technical University, Ankara, Turkey. He is currently the Head of the Security Standardization, Nokia. He has more than 30 years of industry, university, and public-sector research experience in telecommunications as well as network and information security domains. Embedded software development, systems engineering, network architecture, solutions management, consulting, research and innovation and standardization have been within his scope of activities. He took part in numerous network transformation initiatives, starting from Frame Relay and ATM to MPLS and IP through to 5G and industry 4.0. He had also been active in governance, policy, and strategy work at both national and international levels.