IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 June 2023, accepted 19 June 2023, date of publication 21 June 2023, date of current version 28 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3288338

SURVEY

Security Threats to 5G Networks for Social Robots in Public Spaces: A Survey

SAMSON O. ORUMA[1,2] **AND SLOBODAN PETROVIĆ**[2]
[1]Department of Computer Science and Communication, Østfold University College, 1757 Halden, Norway
[2]Institute for Information Security and Communication Technology, Norwegian University of Science and Technology, 2815 Gjøvik, Norway

Corresponding author: Samson O. Oruma (samsonoo@hiof.no)

This work was supported by the Norwegian Research Council through the SecuRoPS Project "User-Centered Security Framework for Social Robots in Public Spaces" under Grant 321324.

ABSTRACT This paper surveys security threats to 5G-enabled wireless access networks for social robots in public spaces (SRPS). The use of social robots (SR) in public areas requires specific Quality of Service (QoS) planning to meet its unique requirements. Its 5G threat landscape entails more than cybersecurity threats that most previous studies focus on. This study examines the 5G wireless RAN for SRPS from three perspectives: SR and wireless access points, the ad hoc network link between SR and user devices, and threats to SR and users' communication equipment. The paper analyses the security threats to confidentiality, integrity, availability, authentication, authorisation, and privacy from the SRPS security objectives perspective. We begin with an overview of SRPS use cases and access network requirements, followed by 5G security standards, requirements, and the need for a more representative threat landscape for SRPS. The findings confirm that the RAN of SRPS is most vulnerable to physical, side-channel, intrusion, injection, manipulation, and natural and malicious threats. The paper presents existing mitigation to the identified attacks and recommends including physical level security (PLS) and post-quantum cryptography in the early design of SRPS. The insights from this survey will provide valuable risk assessment and management input to researchers, industrial practitioners, policymakers, and other stakeholders of SRPS.

INDEX TERMS Social robots, 5G, threat landscape, security, privacy, centralised ledger databases, multi-access edge computing (MEC).

I. INTRODUCTION

The rapid growth of the Internet of Things (IoT), Artificial Intelligence (AI), Robotics, and the emergence of 5G wireless technology have brought about a new era of connectivity, enabling a wide range of applications, including the deployment of Social Robots in Public Spaces (SRPS). Social robots (SR) are becoming increasingly popular in various public spaces, including shopping malls, airports, museums, and hospitals. They are used for multiple tasks, such as guiding visitors, providing information, and entertainment [1]. While SRPS offer numerous benefits, such as enhancing customer experience and reducing human workload, they also introduce new security challenges. Deploying SRPS requires high trust and confidence in their ability to operate safely and securely without threatening the public. Security breaches in SR can have severe consequences, ranging from financial losses to the endangerment of human lives [2].

5G wireless technology is expected to provide advanced services and applications, including SRPS, with higher data rates, lower latency, and increased capacity [3]. However, it also introduces security threats to SRPS. The 3rd Generation Partnership Project (3GPP) has identified service robots with ambient intelligence as a particular use case representing SRPS that needs to be addressed in upcoming studies of 5G Advanced (Release 19) [4]. As standardization efforts for the SRPS use case continue, it is crucial to identify potential threats. Understanding the threat vectors, vulnerabilities, and existing mitigation strategies for SRPS is essential in developing machine-understandable solutions

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

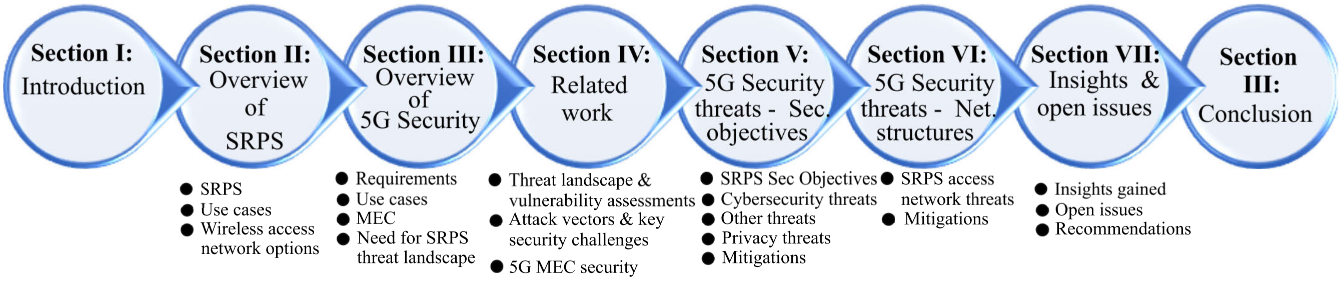
Section I: Introduction
Section II: Overview of SRPS
● SRPS
● Use cases
● Wireless access network options
Section III: Overview of 5G Security
● Requirements
● Use cases
● MEC
● Need for SRPS threat landscape
Section IV: Related work
● Threat landscape & vulnerability assessments
● Attack vectors & key security challenges
● 5G MEC security
Section V: 5G Security threats - Sec. objectives
● SRPS Sec Objectives
● Cybersecurity threats
● Other threats
● Privacy threats
● Mitigations
Section VI: 5G Security threats - Net. structures
● SRPS access network threats
● Mitigations
Section VII: Insights & open issues
● Insights gained
● Open issues
● Recommendations
Section III: Conclusion

FIGURE 1. The structure of this study.

to these problems. Security and privacy concerns are among the main factors that influence users' trust, acceptance, and investors' interest in SRPS [2], [5], [6]. Given the wealth of data collected by SRPS and their proximity to users without supervision, they will attract more threat actors. For example, a malicious actor could compromise the core software of SRPS using a USB pen drive if its ports are accessible [7].

Several studies have investigated the cybersecurity threats to 5G networks from various perspectives, including threat landscape and vulnerability assessment [8], [9], [10], attack vectors and key security challenges [11], [12], [13], and 5G Multi-Access Edge Computing (MEC) Security [14], [15]. However, SRPS use cases face additional threats beyond cybersecurity, such as physical, social, public space, and supply chain threats, which have received limited attention in previous studies [2]. The 3GPP security architecture and procedures for the 5G system are based on studies that did not consider the unique nature of SRPS use cases. Unlike Augmented Reality/Virtual Reality (AR/VR) use cases that require higher traffic in the downlink of a 5G network, SRPS requires more traffic in its uplink due to the massive data collected from the environment to be processed at the 5G MEC as SRPS are power-constrained devices. Data collected by SRPS includes audio, video, sensor, location, and user data.

SRPS have more physical space, enabling them to handle some computation without cloud infrastructure support. This feature makes them capable of handling high-level cryptographic primitives, such as lightweight post-quantum cryptographic algorithms [16], unlike conventional IoT devices. Furthermore, adopting a specific enabling technology can simplify the heterogeneity of 5G RAN for an SRPS application, reducing the complexity associated with its cybersecurity threat landscape.

This paper aims to comprehensively examine the security threats to 5G networks for SRPS to assist researchers, industrial practitioners, policymakers, and other stakeholders in developing effective security solutions for SRPS. Our study identifies the potential threats to the SRPS use case beyond cybersecurity threats and highlights the need for special QoS requirements design of 5G networks. We also present mitigations to identified threats based on best practices and related research.

This paper makes the following contributions:

1) We present a comprehensive survey of the security threats to 5G networks for SRPS, including threats beyond cybersecurity, such as physical, social, public space, and supply chain threats.
2) We summarise the current limitations of the 5G network security architecture for SRPS use cases.
3) We highlight the need for unique Quality of Service (QoS) requirements design of 5G networks for SRPS use cases.
4) We present effective mitigations to the identified threats based on best practices and related research.
5) We provide a comprehensive summary of the development and potential uses of centralized ledger databases, namely LedgerDB, GlassDB, SQL Ledger, TAB1, and PReVer, with a special emphasis on their ability to bolster data security and ensure integrity across diverse scenarios, such as SRPS applications in 5G networks.

Figure 1 provides an overview of our study, while Table 1 lists the acronyms used in this paper. The remainder of the article is structured as follows: Section II overviews SRPS use cases and access network requirements. Section III discusses the 5G Advanced security standards, requirements, use cases, and enabling technologies. Section IV presents related work to this study. Section V analyses the security threats and mitigations to SRPS 5G networks based on its security objectives. Section VI deals with the same subject but is based on the structure of the access network. Section VII recapitulates the insights gained and open research issues. Finally, Section VIII concludes the paper.

II. OVERVIEW OF SOCIAL ROBOTS IN PUBLIC SPACES: USE CASES AND ACCESS NETWORK TYPES

A. SOCIAL ROBOTS IN PUBLIC SPACES

Social robots are AI-powered robots capable of emotional and social interaction with humans while adhering to the social norms expected of the human entities they represent [17]. Social humanoids exhibit five key properties [18]: (i) *physical embodiment* (anthropomorphic or non-anthropomorphic), (ii) *autonomous navigation and decision-making* (without scripting or external control by a human operator), (iii) the ability to *navigate* and freely *interact* with humans and machines, (iv) the ability to *sense and respond* to both human and environmental cues, and (v) the ability to *understand*

TABLE 1. Acronym definitions used in this Study.

Acronyms	Definitions	Acronyms	Definitions
3GPP	3rd Generation Partnership Project	MITM	Man-in-the-Middle
5G	5th Generation	MME	Mobility Management Entity
5G NSA	5G Non-Standalone	mMIMO	Massive MIMO
5GC	5G Core Network	mMTC	Massive Machine-Type Communication
5G-RAN	5G Radio Access Network	mmWave	millimeter Wave
ABAC	Attribute-based Access Control	N3IWF	Non-3GPP access InterWorking Function
ACID	Atomicity, Consistency, Isolation and Durability	NAS	Non Access Stratum
AES	Advanced Encryption Standard	NB-IoT	Narrow Band IoT
AI	Artificial Intelligence	NEA	New radio Encryption Algorithm
AKA	Authentication and Key Agreement	NFC	Near Field Communication
AMF	Access and Mobility Management Function	NFV	Network Function Virtualization
AN	Access Network	NGMN	Next Generation Mobile Networks (Alliance)
API	Application Programming Interface	NIA	New radio Integrity Algorithm
APT	Advanced Persistent Test	NIST	National Institutes for Standards and Technology
AUSF	Authentication Server Function	NR	New Radio
AV	Autonomous Vehicles	NRF	Network Repository Function
bAMT	binary Accumulating Merkle Tree	NS	Network Slicing
BLE	Bluetooth Low Energy	PDCP	Packet Data Convergence Protocol
CAPIF	Common API Framework	PIR	Private Information Retrieval
CC	Cloud Computing	PKI	Public key infrastructure
cC	Cloudlet Computing	PLDs	Permissioned Ledger Databases
CDMA	Code Division Multiple Access	PLMN	Public Land Mobile Networks
CIA	Confidentiality, Integrity, and Availability	Pr	Programmability
CLDs	Centralised Ledger Databases	PUF	Physical Unclonable Function
CLT	Centralised Ledger Technology	QLDB	Quantum Ledger Database
CR	Cloud-RAN	RAN	Radio Access Network
CTR	Counter (mode)	RFID	Radio Frequency Identification
D2D	Device-to-device	RRC	Radio Resource Control
DDoS	Distributed Denial of Service	SBA	Service Based Architecture
DoS	Denial of Service	SC	Small Cells
E2E	Equipment-to-Equipment	SCA	Side Channel Attacks
EAP	Extensible Authentication Protocol	SDN	Software Defined Networking
eMBB	Enhanced Mobile Broadband	SE	Spectral Efficiency
eNB	Evolved Node B	SEPP	Security Edge Protection Proxy
EPC	Evolved Packet Core	SIDF	Subscription Identifier De-concealing Function
EPS	Evolved Packet System	SLA	Service Level Agreements
EU	European Union	SM	Seamless Mobility
FAM	Fractal Accumulating Model	SMC	Secure Multiparty Computation
FIPS	Federal Information Processing Standards	SMF	Session Management Function
Fl	Flexibility	SMS	Short message service
GDPR	General Data Protection Regulation	SR	Social Robots
gNB	NR Node B	SRPS	Social Robots in Public Spaces
GPS	Global Positioning by Satellite	SSL	Secure Socket Layer
GSMA	Global System for Mobile Communications Association	SUCI	Subscription Concealed Identifier
GTP	GPRS Tunnelling Protocol	SUPI	Subscription Permanent Identifier
GUTI	Globally Unique Temporary UE Identity	TABI	Trust-Based ABAC in Edge IoT
HDR	High Data Rates	TLS	Transport Layer Security
HetNet	Heterogeneous Network	TPM	Trusted Platform Manager
IETF	Internet Engineering Task Force	TSA	Timestamp Authority
IKE	Internet Key Exchange	UAV	Unmanned Aerial Vehicle
IMSI	International Mobile Subscriber Identity	UDM	Unified Data Management
IMT	International Mobile Telecommunications	UE	User Equipment
iOS	iPhone Operating System	uLL	Ultra-Low Latency
IoT	Internet of Things	UP	User Plane
IPSec	Internet Protocol Security	UPF	User Plane Function
LiFi	Light Fidelity	uRA	Ultra-Reliability and Availability
M2M	Machine-to-Machine	uRLLC	Ultra-Reliable, and Low Latency Communication
MANET	Mobile Ad-hoc Network	WAN	Wireless Access Network
MANO	Management and Network Orchestration	WebOS	Web Operating System
MC	Massive Connectivity	WiMAX	Worldwide Interoperability for Microwave Access
MEC	Multi-access Edge Computing	WLAN	Wireless Local Area Network
MIMO	Multiple-Input, Multiple-Output		

and comply with applicable social norms (expected societal rules). At a technical level, SR should possess the following features [19]: (i) **Perception** (including vision, hearing, smell, touch, and reflexes), (ii) **Cognition** (incorporating emotional, social, and motor planning through machine learning), (iii) **Action** (including tool handling, movable joint control, and prosthetic devices) (iv) **Interaction** (with humans, gestures, and maintaining acceptable proximity to

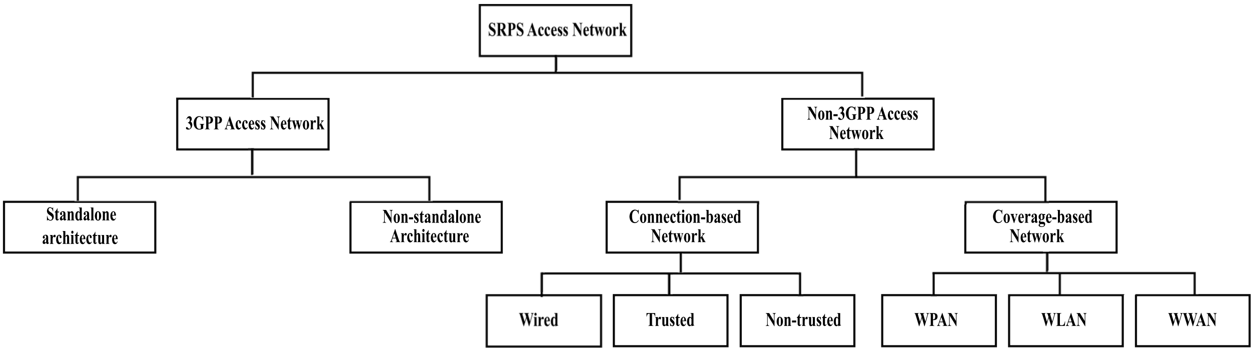

FIGURE 2. Wireless access network options for SRPS.

users [20]), (v) **Efficiency** (in terms of energy, time, cost, and regulatory compliance), (vi) **Ethics** (compliance with regulatory laws, proper usage, i.e., not being used as a weapon, ensuring safety and security during operation, and being solely responsible to a human user).

Social robots have seven sub-components [2]: hardware, software, communication, cloud services, AI services, supply chain, and human. SRPS is an emerging trans-disciplinary field involving cognitive science, social science, AI, computer science, human-computer interaction (HCI), psychology, engineering, and robotics [21].

In the context of this study, **public space** refers to privately and publicly owned indoor or outdoor areas that are generally accessible to all individuals, regardless of gender, race, ethnicity, age, or socio-economic status [22], [23]. Access may be limited during specific times of the day (e.g., in shopping malls, hospitals, elderly care homes, museums, etc.). Laws, culture, and institutional norms highly regulate public places, so acceptable behaviours and activities are expected in these locations [24]. It is anticipated that SR will soon operate freely (without supervision) in such spaces, implying that users and threat actors will have unsupervised access to these social humanoids. Public places are subject to unexpected and dynamic natural (environmental) and human factors. Changes in environmental factors, such as rain or wind, can affect the wireless access connections of SRPS. SR must adhere to societal standards and exhibit expected behaviour while operating in public settings, as people ascribe value to a place based on their experiences and the quality of interactions received [25].

B. SOCIAL ROBOT USE CASES FOR PUBLIC SPACES

We envision a future where SR play a vital role in our daily lives. At least one SR in each home provides services such as cleaning, cooking, and handling repetitive human tasks, allowing humans to focus on more important tasks. The list of practical and viable use cases for SRPS is extensive. Still, this study will consider the following four domains from previous research: education, healthcare, services, and entertainment.

1) EDUCATION

Several studies have explored the potential of using SR in education. SR can serve as tutors [26], teaching assistants [27] for distance learning involving children with Autism Spectrum Disorder (ASD) [28], early language tutors for children [29], youths, and adults [30], and secondary language tutors [31].

2) HEALTHCARE

Healthcare presents numerous potential use cases for SRPS, including: (i) Providing engaging and therapeutic companionship for hospitalized children [32], (ii) Offering psychosocial health interventions for patients [33], (iii) Serving as a valuable tool for depression management in smart homes for elderly care [34], (iv) Aiding in mental health and well-being management for older adults [35], (v) Providing personal support for senior citizens living with disabilities and dementia [36].

3) SERVICES

Service-related use cases encompass SR functioning as receptionists [37], museum guides [38], hotel waiters/bartenders [39], retail service providers, multi-channel public service delivery agents [40], catering services [41], and corporate brand strategists for organizations [42].

4) ENTERTAINMENT

SR can be employed as cyber-physical actors in entertainment [43] and theatre arts [44]. Another potential use case is providing companionship for senior citizens with sexual disabilities [45].

C. WIRELESS COMMUNICATION ACCESS NETWORK OPTIONS FOR SRPS

The 5G access network options available to SRPS, as specified by the 3GPP [46], can be grouped into 3GPP access and non-3GPP access networks, as summarized in Figure 2.

The 3GPP access can take the form of a non-standalone architecture (which incorporates earlier communication technologies like 4G or 3G) or a standalone 5G architecture purely

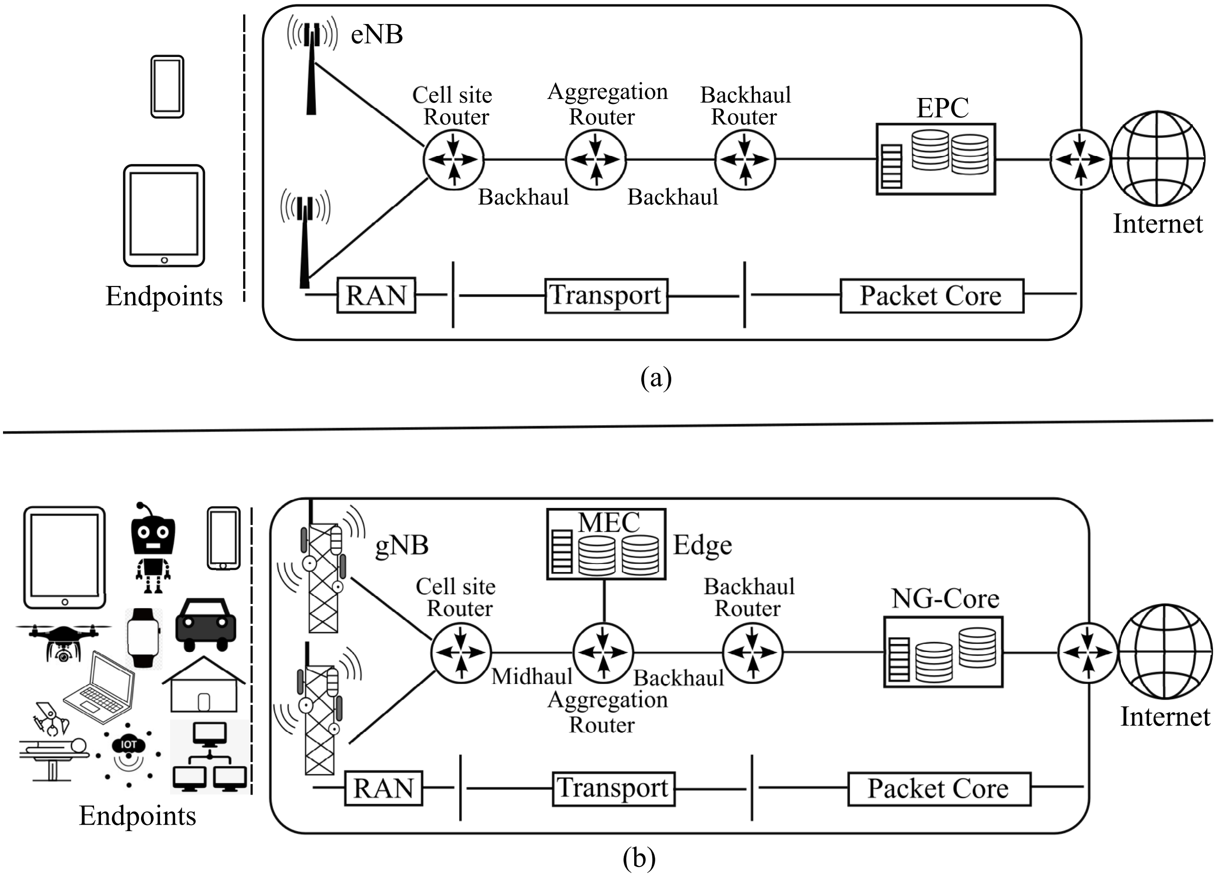

FIGURE 3. Overview of end-to-end access network options for SRPS (a) LTE (b) 5G.

based on 5G technology. Non-3GPP access can further be categorized based on connection trust level (wired, trusted, and untrusted) or geographical coverage of the network (WPAN, WLAN, and WWAN). Due to the autonomous mobile nature of SR, a wired connection is not a suitable option for consideration in this use case.

A high-level overview of the 3GPP access network for LTE and 5G NR is presented in figure 3. It consists of five main components; Endpoints, RAN, Transport, Packet Core and Internet. Endpoints represent end users' devices, which for LTE are mobile phones with internet capabilities connected to the eNBs. The RAN is where endpoints connect to antennas (eNB for LTE and gNB for 5G NR) and where antennas connect to the backhaul of the network.

In traditional telecommunication settings, RAN consists of a cell tower (a fixed infrastructure that facilitates wireless communication between the user equipment and the core network) and a base station with the following resources; (1) **Antennas** which are responsible for transmitting and receiving radio frequency (RF) signals between the user equipment and the base station. They are typically mounted on a tower, pole, or rooftop to ensure optimal signal coverage. (2) **Remote Radio Units - RRU** which are responsible for converting the received RF signals to digital signals and vice versa. They are usually located near the antennas to minimize signal loss. (3) **Baseband Units - BBUs** which consists of dedicated hardware that processes the digital signals received from the RRUs, performing functions such as error correction, modulation, and encoding. BBUs then route the processed signals to the core network through the backhaul. In some configurations (LTE), BBUs are moved to a central location (Centralised RAN) using long fibre optics cables (CPRI for LTE and eCPRI for 5G) between RRU (i.e. RE for LTE and eRE for 5G) and the centralized RAN (REC for LTE and eREC for 5G). (4) **Backhaul** which refers to the wired or wireless connection between the base station and the core network. It is responsible for transmitting data to and from the base station. Common backhaul technologies include fibre-optic cables, microwave links, and satellite links. (5) **Power supply** a reliable power supply is essential for the continuous operation of the base station. It can be in the form of direct electricity from the grid, batteries, solar panels, or a combination of these sources. Backup power sources, such as generators, are often installed to ensure uninterrupted service during power outages. (6) **Cooling and climate control system** helps maintain optimal temperatures within the equipment enclosure, ensuring the proper functioning and longevity of the electronic components. (7) **Monitoring and control systems** These systems allow network operators to remotely monitor and manage the base station's performance, perform maintenance, and diagnose any issues that may arise.

Today, modern RAN are virtualized (vRAN), which represents the transition of BBUs to software that runs on commercial-off-the-shelf (COTS) hardware. This enables the task of the BBU to be carried out at the software level in the form of virtual network functions (VNFs). Centralized RAN (C-RAN) is a 5G network architecture that centralizes the processing and baseband functions of multiple remote radio units (RRUs) into a single baseband unit (BBU) pool. This architecture offers several advantages for 5G networks [12]: (i) **Improved spectral efficiency:** By centralizing the baseband processing, C-RAN enables more efficient use of the available spectrum, leading to higher capacity and improved data rates. (ii) **Enhanced coordination and interference management:** In a C-RAN architecture, centralized processing allows for better coordination between multiple RRUs. This results in improved interference management and increased network capacity. (iii) **Reduced latency:** With the centralized processing of baseband functions, C-RAN can reduce the latency of the fronthaul network, which is crucial for supporting ultra-low latency 5G applications. (iv) **Lower Total Cost of Ownership (TCO):** Centralizing the baseband processing can lead to cost savings due to reduced infrastructure requirements, power consumption, and operational costs. This reduction in TCO can make 5G networks more economically viable for network operators. (v) **Increased scalability and flexibility:** C-RAN architecture is more scalable and flexible than traditional distributed RAN architectures. This allows for easier network expansion and upgrades and more efficient resource allocation and management.(vi) **Enhanced energy efficiency:** By consolidating baseband processing in a single location, C-RAN can reduce the overall energy consumption of the network, leading to a more environmentally friendly and cost-effective solution. (vii) **Improved network reliability:** Centralizing the baseband functions allows for better fault detection, isolation, and recovery, leading to increased network reliability and resilience. (viii) **Simplified network management:** C-RAN enables centralized network management and control, resulting in simplified operations and maintenance.

The transport section of a 5G network refers to the part of the network responsible for transmitting data between different components, such as radio access network (RAN) elements and the core network. The transport section typically consists of the fronthaul, mid-haul, and backhaul segments, and various components, devices, and protocols are involved in its functioning [47]:

1) **Fronthaul** This segment connects the remote radio units (RRUs) or remote radio heads (RRHs) to the centralised baseband units (BBUs) or centralised RAN (C-RAN) processing pool [48]. Common fronthaul interfaces and protocols include: (i) Common Public Radio Interface (CPRI) [49], (ii) Enhanced Common Public Radio Interface (eCPRI) [50], and (iii) Open Radio Access Network (O-RAN) Fronthaul Interface [51].
2) **Midhaul** This segment connects the centralised BBUs or distributed units (DUs) to the centralised control units (CUs) in the RAN [52]. It is also known as the "X2" interface in the LTE architecture. Protocols used in the mid-haul segment include: (i) S1/X2 Application Protocol (S1AP/X2AP), and (ii) Packet Data Convergence Protocol (PDCP)
3) **Backhaul** This segment connects the RAN elements (BBUs, DUs, or CUs) to the core network elements [53]. The backhaul segment typically involves various transport technologies and protocols, including (i) Internet Protocol (IP), (ii) Multi-Protocol Label Switching (MPLS), (iii) Ethernet, (iv) Optical Transport Network (OTN), (v) Time-sensitive networking (TSN), (vi) Microwave and millimetre-wave (mmWave) links for wireless backhaul, and (vii) Software-Defined Networking (SDN) for efficient network control and management.
4) **Synchronisation:** Accurate time synchronisation is crucial in 5G networks, especially for TDD (Time Division Duplex) operation and massive MIMO (Multiple-Input Multiple-Output) technologies [54]. Synchronisation protocols include: (i) Precision Time Protocol (PTP) or IEEE 1588 and (ii) Synchronous Ethernet (SyncE)

The transport also consists of routers and aggregate routers that forward packets using protocols such as MPLS, BGP, and SRV6. The packet core (EPC for LTE or NG-Core for 5G) is a central server or multiple data centres that connects to the internet.

In 5G (Figure 3b), there are several enhancements as follows; (i) The endpoints accommodate more use cases and devices such as smart watches, autonomous vehicles, IoT (smart farm), drones, robots, smart homes, mission-critical applications like telesurgery, etc., (ii) the 5G antennas (gNB) has more enhancements in terms of spectral efficiency, new spectrum allocation, and technologies (e.g. mmMave), while Res and RECs also evolved to eREs and eRECs, respectively, (iii) enhancement in the connection link between RE and REC from CPRI to eCPRI on which IQ data is sent. (iv) Enhancement in the functional split of the RAN architecture into distributed units (DU) and centralized units (CU), thereby moving some processing functions to the fronthaul of the network; with the introduction of MEC, some CU operations are conducted on the edge of the network to meet specific use cases such as low latency. (v) the introduction of O-RAN architecture leading to interoperability standards between different RAN vendors to promote openness, diversity in numbers of vendor actors, specialization and ultimately cost reduction in RAN hardware.

TABLE 2. A list of key security specifications by 3GPP SA WG3.

		First version		Current version*		No. of
TS/TR	Description	Version	Date	Version	Date	Revisions
TS 33.501 [46]	Security architecture and procedures for 5G systems	15.1.0	2018-06	18.0.0	2022-12	589
TS 33.117 [55]	Catalogue of general security assurance requirements	14.1.0	2016-12	17.2.0	2022-12	37
TS 33.511 [56]	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network protocol class	0.0.0	2018-09	17.3.1	2023-02	24
TS 33.512 [57]	5G SCAS: Access and mobility management function (AMF)	16.0.0	2019-09	17.3.0	2022-03	17
TS 33.513 [58]	5G SCAS; User Plane Function (UPF)	0.0.0	2018-08	17.1.0	2023-01	15
TS 33.514 [59]	5G SCAS for the Unified Data Management (UDM) network product class	0.1.0	2018-09	17.0.0	2021-06	15
TS 33.515 [60]	5G SCAS for the Session Management Function (SMF) network product class	0.0.0	2018-09	17.0.0	2022-03	15
TS 33.516 [61]	5G SCAS for the Authentication Server Function (AUSF) network product class	0.1.0	2018-11	17.0.0	2022-03	10
TS 33.517 [62]	5G SCAS for the Security Edge Protection Proxy (SEPP) network product class	0.1.0	2018-11	17.0.0	2021-06	14
TS 33.518 [63]	5G SCAS for the Network Repository Function (NRF) network product class	0.1.0	2018-11	17.0.0	2022-03	12
TS 33.519 [64]	5G SCAS for the Network Exposure Function (NEF) network product class	0.1.0	2018-10	17.0.0	2022-03	13
TS 33.520 [65]	5G SCAS; Non 3GPP InterWorking Function (N3IWF)	0.0.0	2020-05	0.3.0	2021-12	5
TS 33.521 [66]	5G SCAS; Network Data Analytics Function (NWDAF)	0.0.0	2020-05	17.2.0	2022-06	9
TS 33.522 [67]	5G SCAS; Service Communication Proxy (SECOP)	0.0.0	2020-05	17.1.0	2022-03	8
TR 33.842 [68]	Study on Lawful Interception (LI) service in 5G	0.0.0	2017-11			0
TS 33.126 [69]	Lawful Interception requirements	16.0.0	2019-06	18.0.0	2022-09	10
TS 33.127 [70]	Lawful Interception (LI) architecture and functions	16.11.0	2022-06	18.2.0	2022-12	12
TS 33.128 [71]	Security; Protocol and procedures for Lawful Interception (LI); Stage 3	16.3.0	2022-12	18.2.0	2022-12	12
TR 33.811 [72]	Study on security aspects of 5G network slicing management	0.2.0	2017-11	15.0.0	2018-06	7
TR 33.839 [73]	Study on security aspects of enhancement of support for edge computing in 5GC	0.0.0	2020-08	17.1.0	2022-03	13
TR 33.819 [74]	Study on security enhancements of 5G System (5GS) for vertical and LAN services	0.0.0	2018-11	16.1.0	2020-07	13
TR 33.809 [75]	Study on 5G security enhancements against False Base Stations (FBS)	0.11.0	2020-10	0.20.0	2022-10	11
TR 33.853 [76]	Key issues and potential solutions for integrity protection of the User Plane (UP)	0.0.0	2019-02	17.0.0	2021-06	19
TR 33.846 [77]	Study on authentication enhancements in the 5G System (5GS)	0.1.0	2019-04	17.0.0	2021-12	8
TS 33.818 [78]	SECAM and SCAS for 3GPP virtualised network products	0.0.0	2018-11	17.1.0	2021-09	18
TS 33.187 [79]	Security aspects of MTC and other mobile data applications communications enhancements	0.1.0	2013-04	17.0.0	2022-03	16
TS 33.303 [80]	Proximity-based Services (ProSe); Security aspects	0.2.0	2014-05	17.1.0	2022-09	17
TS 33.536 [81]	Security aspects of 3GPP support for advanced V2X services	0.0.0	2020-02	17.1.0	2022-06	16
TS 33.535 [82]	Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in 5GS	0.0.1	2019-10	17.7.0	2022-09	19
TS 33.122 [83]	Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs	0.1.0	2018-01	17.1.0	2023-01	14

* Version in effect as of March 2023

III. OVERVIEW OF 5G SECURITY STANDARDS

The primary standardizing body for 5G security is the 3GPP, which collaborates with other international and regional organizations such as ETSI, IETF, IEEE, ITU-T, GSMA, NGMN, and 5GPPP. Standards play a crucial role in ensuring the security, interoperability, and openness of 5G networks through commonly agreed-upon, tested, verified, and updated solutions. The 3GPP unifies global telecommunications standards with specific emphasis on (i) cellular communication, (ii) radio access network, (iii) non-radio access network, (iv) core network, and (v) inter-working with non-3GPP networks. 3GPP has seven organizational partners, 28 market representative partners, and two observers [84].

Internally, 3GPP operates through the following working groups [85]: (i) Core Network and Terminal (CT) – 4 groups, (ii) Radio Access Network (RAN) – 6 groups, (iii) Service and System Aspect (SA) – 6 groups, (iv) a Project Coordination Group, and (v) a closed group. The group responsible for defining and specifying the architectures and protocols for security and privacy in 3GPP systems is SA WG3. This group conducts studies and collaborates with other 3GPP partners to publish technical specifications and reports (TS/TR) that constitute 5G security standards upon freezing. Most of these publications are under change control as they continuously undergo improvement from stakeholders and reviews. Table 1 presents the various technical specifications and reports published by SA WG3 of the 3GPP.

The security architecture and procedures [46], defined by 3GPP SA3, encompass security solutions from several standardization organizations. The IETF defines security

TABLE 3. A list of 5G security domains.

#	Security domain	Description
1	Network Access Security	Inherent security features enabling User Equipment (UE) to authenticate and access services through the network. This involves the following six links: (i) USIM and ME, (ii) USIM and SN, (iii) ME and AN (3GPP-AN and Non-3GPP-AN), (iv) ME and SN, and (v) SN and HE.
2	Network Domain Security	Inherent security features enable network nodes to exchange signalling and user plane data securely. This involves the following links: (i) AN and SN, (ii) SN and HE.
3	User Domain Security	The inherent security features ensure secure access between USIM and ME, thereby securing user access to mobile equipment.
4	Application Domain Security	Inherent security features that enable secure exchange of messages between user applications and service provider applications.
5	SBA Domain Security	The group of security tools that allow SBA architecture's network functions to securely communicate within serving network domains. These characteristics include network function registration, discovery, authorisation security elements, and the protection of service-based interfaces. This involves the link between SN and HE.
6	Visibility and Configuration of Security	Inherent security features that inform users of the presence or absence of certain security features.

protocols such as IPsec, OAuth 2.0 authorization framework, Extensible Authentication Protocol (EAP), Hypertext Transfer Protocol version 2 (HTTP/2), Internet Key Exchange protocol version 2 (IKEv2), and Transport Layer Security (TLS), all of which are incorporated into the 5G security architecture. The 5G core network utilizes cloud and virtualization technologies, with ETSI ISG NFV defining security for network functions virtualization (NFV) [59]. The National Institute for Standards and Technology (NIST) standardizes cryptographic solutions such as AES, and the recently approved NESAS framework for security assurance is a joint effort between 3GPP SA3 and GSMA. ITU-T SG 17 has developed X-series security recommendations on SDN, NFV, IoT, big data analytics in mobile internet services, cloud computing, and cryptographic profiles, which are also incorporated into the 5G security architecture [60]. All these different components collectively form the security standard for 5G.

5G security standards are driven by the priority use cases of 3GPP partners, which primarily focus on cellular communication [86]. The standardization effort is more directed towards 3GPP access technologies, while non-3GPP access technology specifications allow for diverse integration at the implementation and design stages. SRPS, as an emerging research direction, is not covered in the first phase of 5G standardization or included enhancement/vertical. 3GPP is directing future research efforts to study networks for service robots with ambient intelligence (FS_SOBOT) [4], related to the SRPS use case in the upcoming Release 19. The threat landscape for this use case is essential for sound security standardization.

1) SECURITY REQUIREMENTS IN 5G NETWORK

The 5G advanced security architecture, as specified by 3GPP in Release 18 [30], consists of six security domains, as presented in Table 3. The inbuilt security system for 5Gs is designed to meet the following requirements:

a: MUTUAL AUTHENTICATION AND AUTHORIZATION

Mutual authentication involves the UE authenticating the service network identifier through implicit key authentication, while the serving network verifies the legitimacy of the UE (subscription authentication) through SUPI during the 5G AKA process. The AUSF serves as a liaison between the AMF and UDM for the 5G AKA process, while the UDM generates the primary 5G authentication vector. The serving network authorizes the UE based on the SUPI subscription profile obtained from the home network. In contrast, the UE receives serving network and access network assurance through authorization from the home network following a successful authentication and key agreement run. The system also supports unauthenticated emergency services, especially in regions where emergency services require no authentication.

b: CIPHERING AND INTEGRITY PROTECTION

5G supports ciphering (encryption) of RRC signalling, NAS signalling, and user plane data to ensure the confidentiality of such data between the ME, gNB, and AMF, using appropriate ciphering algorithms (NEA0, 128-NEA1, 128-NEA2, or 128-NEA3). The system provides separate keys for ciphering and integrity protection. However, confidentiality protection is optional and subject to regulatory approval. The standard also requires the UE to support the integrity and replay protection of data (RRC, NAS signalling, and user data) between the UE, gNB, and AMF. Integrity protection is mandatory, except for user plane data subject to specific use cases.

c: PROTECTING SERVICE-BASED ARCHITECTURE

5G supports two optional security features for protecting SBA infrastructure: (i) the use of Transport Layer Security (TLS 1.2 and above) to protect HTTP messages in the SBA, and (ii) the use of OAuth 2.0 token-based authentication, along with public key infrastructure services, to protect the SBA against malicious service requests.

d: ROAMING PROTECTION

5G employs three security features for roaming protection – SEPP, PRINS, and IPUPS. The Security Edge Protection Proxy (SEPP) is responsible for security-related tasks such as topology hiding, message filtering, and traffic policing. When there is a third-party connection between the home PLMN and the visited PLMN through the N32 channel, another security feature (Protocol for N32 Interconnect Security – PRINS) is used. PRINS ensures data integrity protection while allowing the IPX network to make forwarding changes to the packet without compromising integrity. The Inter

PLMN User Plane Security (IPUPS) ensures that all N9 traffic goes through a GPRS Tunneling Protocol (GTP) tunnel, thereby protecting against injected traffic attacks.

e: PROTECTION OF SUBSCRIBER'S IDENTITY

In 5G, the subscriber's identity is protected through SUCI (Subscription Concealed ID), which is generated from the IMSI and public key encryption process. The MCC and MNC of the SUCI may be transmitted in plain text, but its MSIN component is encrypted to protect the subscriber's identity. Unlike earlier communication technologies, where the IMSI must be transmitted after a long period of service disconnection with the UE, the IMSI in 5G networks is always protected.

A. OVERVIEW OF 5G USE CASES, KEY REQUIREMENTS AND ENABLING TECHNOLOGIES

5G networks are designed to support a wide range of use cases, addressing various industry sectors and improving existing services. Some of the key use cases for 5G networks include:

1) **Enhanced Mobile Broadband (eMBB):** 5G aims to provide faster data speeds, lower latency, and higher network capacity, enabling high-quality video streaming, virtual reality (VR), augmented reality (AR), and other bandwidth-intensive applications on mobile devices [87].
2) **Massive Machine-Type Communications (mMTC):** 5G is designed to support the massive number of devices expected in the IoT ecosystem, which includes smart cities, smart homes, smart industries, and other large-scale IoT deployments. mMTC allows for low-power, low-data-rate communication between devices, enabling extended battery life and efficient network resource utilization [88].
3) **Ultra-Reliable Low-Latency Communications:** 5G enables critical applications that require extremely low latency and high reliability, such as autonomous vehicles, industrial automation, remote surgery, and smart grids. URLLC allows for near-instantaneous communication between devices, with minimal delays and high levels of reliability [89].
4) **Vehicle-to-Everything (V2X) Communications:** 5G supports improved communication between vehicles and other elements of the transportation infrastructure (e.g., traffic lights, road signs, pedestrians, and other vehicles). This enhanced connectivity enables various applications like cooperative driving, traffic management, and improved road safety [90].
5) **Smart Cities:** 5G networks can support the development of smart cities by connecting various urban systems and infrastructures, such as transportation, energy, water, and waste management. This connectivity enables better resource management, improved quality of life for residents, and more sustainable urban environments [91].
6) **Industrial IoT and Automation:** 5G networks enable Industry 4.0 applications, such as real-time monitoring and control of manufacturing processes, robotics, and logistics [92]. These applications require high reliability, low latency, and secure communication, which 5G can provide.
7) **Remote Healthcare:** 5G networks can improve telemedicine and remote healthcare services by enabling high-quality video consultations, remote patient monitoring, and even remote surgery. These applications require reliable, low-latency communication and high data rates [93].
8) **Entertainment and Gaming:** 5G enhances the entertainment and gaming industries by enabling high-quality video streaming, immersive virtual reality experiences, and cloud gaming services with low latency and high data rates [94].
9) **Public Safety and Emergency Services:** 5G can improve the efficiency and effectiveness of public safety and emergency services by providing reliable, real-time communication between first responders, control centres, and other stakeholders [95].
10) **Agriculture and Environmental Monitoring:** 5G networks can support precision agriculture and environmental monitoring applications by providing real-time data on soil conditions, weather, and other factors. This information can help optimize resource use, improve crop yields, and reduce environmental impact [96].

In Release 18, the focus has expanded to include enhanced eMBB, extended reality (XR, including AR and VR), industrial IoT/mMTC, AI/ML-based services, network evolution, satellite communication integration, and public safety/mission-critical services. However, SRPS has not been incorporated into the security design considerations or service assurance evaluations.

The 3GPP [3] and ITU-R [97] have classified the various use cases of 5G-enabled networks into three main categories, featuring 12 essential requirements. These categories are: (i) enhanced mobile broadband (eMBB), (ii) ultra-reliable and low latency communication (uRLLC), and (iii) massive machine-type communication (mMTC), as depicted in Figure 4. Table 4 provides an overview of the essential 5G requirements related to SRPS from both user experience and network management perspectives [98]. The twelve 5G requirements can be grouped into user experience, network management, and hybrid requirements. User experience requirements encompass ultra-low latency (uLL), ultra-reliability and availability (uRA), high data rates (HDR), and seamless mobility (SM). Network/system management requirements include massive connectivity (MC), spectral efficiency (SE), programmability (Pr), and flexibility (Fl). Hybrid requirements, such as enhanced security, privacy, energy, and cost efficiencies, are relevant to users and network management. However, not all of these requirements apply to the SRPS use case.

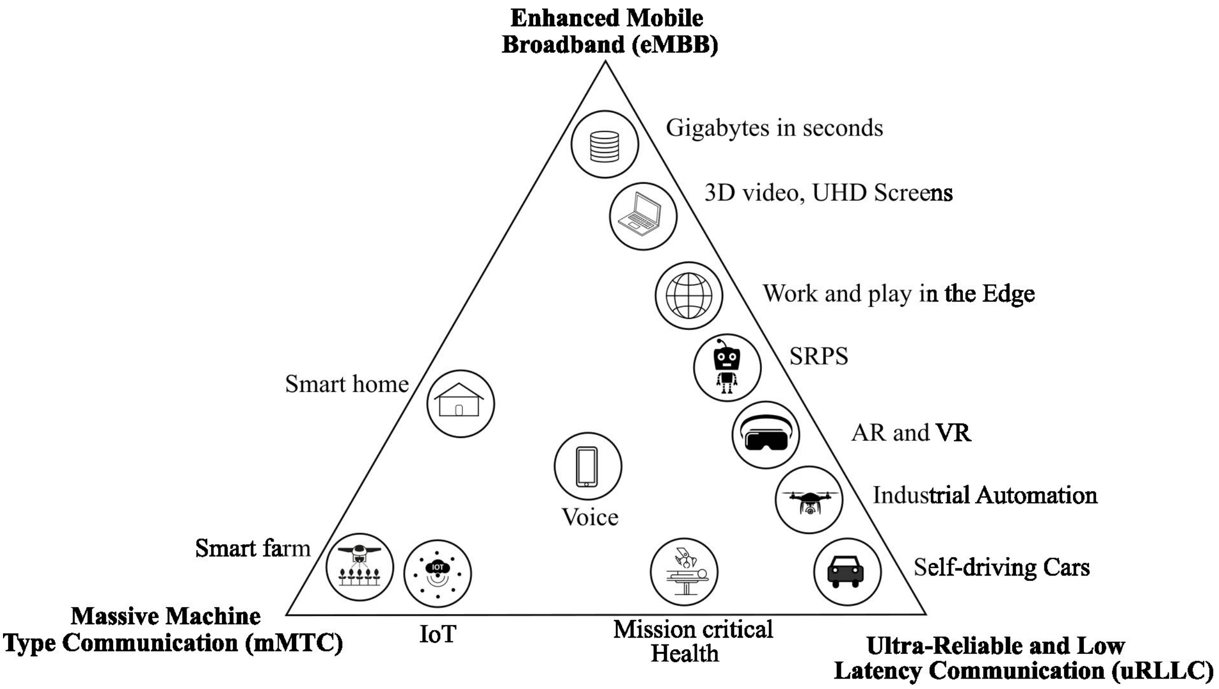
Enhanced Mobile Broadband (eMBB)
Gigabytes in seconds
3D video, UHD Screens
Work and play in the Edge
SRPS
AR and VR
Industrial Automation
Self-driving Cars
Smart home
Voice
Smart farm
IOT
Massive Machine Type Communication (mMTC)
IoT
Mission critical Health
Ultra-Reliable and Low Latency Communication (uRLLC)

FIGURE 4. 5G Use Cases.

TABLE 4. Summary of 5G use cases, key requirements, specifications and enabling technologies from user experience and network management perspectives.

Perspective	Requirements	Applicable to SRPS?	5G specifications	Enabling technologies
User experience	Ultra-low latency	Yes	$1mS$(uRLLC), $4mS$(eMBB)	MEC, cC, D2D, M2M
	Ultra-reliability	Yes	99.999%	NFV, SDN, cC, CR, MANO
	High data rates	Partially (uplink)	Peak rate (20Gbps), user data (1Gbps)	SC, massive MIMO, mmWave
	Seamless mobility	No	500 km/h (speed)	SC, massive MIMO, D2D, M2M, MANO
Hybrid	Enhanced security	Yes	Secure network	NFV, SDN, cC, CR, MANO, NS
	Cost efficiency	Yes	Reduced cost	NFV, SDN, cC, CR, MANO, NS
	Energy efficiency	Yes	$100 \times 4G$	NFV, SDN, cC, CR, MANO, NS
	Enhanced privacy	Yes	Guaranteed privacy	NFV, SDN, cC, CR, MANO, NS
Network mgt.	Spectral efficiency	Yes	$0.12 - 30$bits/s/Hz	NFV, SDN, SC, massive MIMO, D2D, M2M
	Programmability	Yes	Programmable	NFV, SDN, cC, CR, MANO, NS
	Flexibility	Yes	Flexible	NFV, SDN, cC, CR, MANO, NS
	Massive connectivity	No	1000000 nodes km^2	SC, massive MIMO, D2D, M2M

The mMTC use case is not applicable to SRPS, as it focuses on IoT devices with dense connections of about one million nodes per square kilometer. The eMBB use case is only partially related to SRPS because, unlike traditional communication systems for users, uplink data traffic will be more significant than downlink data for this use case. For example, IMT-2020 specifications are 20 Gbps (downlink) and 10 Gbps (uplink) [99], while 3GPP's theoretical data rates are 100 Mbps (downlink) and 50 Mbps (uplink) [100], respectively. SRPS requires more data in the uplink direction than in the downlink.

5G networks employ various enabling technologies to achieve high data rates, ultra-low latency, and massive connectivity, fulfilling their RAN SLAs. These technologies collaborate to create a flexible, high-performance 5G network infrastructure capable of supporting a wide array of use cases and applications. Each enabling technology has its unique characteristics and inherent security vulnerabilities. Some of the key enabling technologies for 5G networks include:

1) **Millimeter-wave (mmWave) communication:** 5G networks utilize higher frequency bands in the millimetre-wave spectrum, significantly increasing data rates and network capacity [101].
2) **Massive MIMO (Multiple-Input Multiple-Output):** This technology uses large antenna arrays at the base station to enhance spectral efficiency, network capacity, and coverage [102].
3) **Beamforming:** This technique directs radio signals towards specific users, improving signal strength, reducing interference, and increasing network capacity [103].
4) **Small cells:** These low-power base stations boost network capacity and coverage by offloading traffic from macro cells, allowing for more efficient use of available spectrum and reduced latency [104].

5) **Network slicing:** This technology enables the creation of multiple virtual networks on a single physical network infrastructure, allowing operators to customize services and resources for different use cases and customer requirements [105].
6) **Edge computing:** By processing data closer to the user, edge computing reduces latency and increases data transmission efficiency, which is essential for supporting ultra-low latency applications like autonomous vehicles and remote surgery [106].
7) **Software-defined networking (SDN) and network function virtualization (NFV):** These technologies separate the network control plane from the data plane, enabling centralized control, improved resource utilization, and more efficient network management [107].
8) **Non-Orthogonal Multiple Access (NOMA):** NOMA is a multiple access scheme that enables multiple users to share the same time-frequency resources, enhancing spectral efficiency and capacity in 5G networks [108].
9) **Device-to-Device (D2D) communication:** D2D communication allows devices to communicate directly with each other without a central base station, improving energy efficiency and reducing latency [109].
10) **Enhanced security:** 5G networks incorporate advanced security measures, including stronger encryption, authentication, and privacy protection mechanisms, to meet the growing demand for secure communication [46].

An efficient security design for 5G-enabled networks for SRPS will guarantee security at three levels: access, infrastructure and service. It will also ensure the security and safety of its enabling technologies [98].

B. MULTI-ACCESS EDGE COMPUTING (MEC) FOR SRPS ACCESS NETWORKS

Social robots operating in public spaces will collect massive amounts of data from users and their environments during interactions. This data will be processed by various computer vision, NLP, and other AI models to inform the decisions of the SR. To meet the expected user experience and service level agreement (SLA), it is essential to process and store the collected big data using a viable edge computing approach. As a 5G enabling technology, Edge computing is crucial to SRPS access networks because it helps reduce latency, improve data transmission efficiency, enhance privacy and security, allow scalability, increase network and energy efficiency, and facilitate better real-time decision-making. These benefits are essential for supporting the wide range of SRPS use cases and applications that 5G networks aim to enable. A brief description of the benefits includes [14]:

- **Reduced latency:** A primary goal of 5G networks is to provide ultra-low latency communication. Edge computing enables data processing closer to users and devices, significantly reducing the time it takes for data to travel between the user and the data centre. This reduced latency is crucial for real-time applications such as autonomous vehicles, remote surgery, augmented reality (AR), virtual reality (VR), and online gaming.
- **Improved data transmission efficiency:** By processing data at the network's edge, edge computing reduces the amount of data that needs to be transmitted to and from centralised data centres. This decreases the load on the network and improves overall transmission efficiency, leading to a more responsive and reliable user experience.
- **Enhanced privacy and security:** Edge computing allows sensitive data to be processed locally, reducing the need to transmit it across the network. This can help minimise the risk of data breaches and unauthorised access. Additionally, edge computing can support localised encryption and security measures, providing extra protection for sensitive data.
- **Scalability:** As the number of connected devices and the amount of data generated by these devices continue to grow, centralising all data processing in the cloud can become increasingly complex and expensive. Edge computing enables a more distributed and scalable approach to data processing, allowing 5G networks to handle the massive amounts of data generated by IoT devices, smart cities, and other applications more efficiently.
- **Network and energy efficiency:** Processing data at the edge can reduce the amount of data that needs to be transmitted over the network, leading to more efficient use of network resources. This can also save energy, as less power is required for data transmission and processing.
- **Better real-time decision-making:** Edge computing enables real-time data analysis and decision-making, which is essential for many applications, such as industrial automation, intelligent transportation, and public safety. By processing data locally, edge computing allows for faster response times, enabling better decision-making and more efficient operation of these systems.

There are several implementation paradigms for 5G edge computing, each with its unique characteristics and advantages. Some of the prominent paradigms include:

1) **Multi-Access Edge Computing (MEC):** MEC [14] is a standardised edge computing architecture that brings computing and storage resources closer to the users and devices. It enables efficient and low-latency data processing from various access networks, such as cellular, Wi-Fi, and wired networks. MEC is highly suitable for integrating 5G technologies and supports many applications, including IoT, augmented reality, and real-time analytics.
2) **Fog Computing:** Fog computing [110] is an extension of cloud computing that distributes data processing, storage, and networking resources closer to the end devices. It forms a decentralised network of fog nodes that can process and analyse data locally, reducing

latency and improving overall network efficiency. Fog computing is beneficial for applications requiring real-time processing and low-latency communication.

3) **Cloudlet Computing:** Cloudlet computing, or mobile edge computing [111], is a specialised form that provides mobile users with low-latency and high-bandwidth access. Cloudlets are small-scale data centres deployed at the network's edge, enabling rapid offloading and processing of tasks from mobile devices. This paradigm is well-suited for applications that require fast response times and high levels of user mobility, such as mobile gaming and virtual reality.
4) **Mist Computing:** Mist computing [112] is a highly decentralised edge computing approach that pushes data processing, storage, and networking resources closer to edge devices. In this paradigm, the edge devices themselves perform the necessary computing tasks, reducing the need for data transmission to centralised data centres or other edge nodes. Mist computing is particularly useful for applications with strict latency requirements, highly distributed networks, or limited network connectivity.

Yousefpur et al. conducted a comprehensive survey of these edge-computing approaches in [110]. Each paradigm provides unique 5G edge computing advantages, catering to varying application requirements and network architectures. The selection of the appropriate paradigm depends on factors such as latency, bandwidth, scalability, and the specific use case. In this study, MEC is recommended due to its suitability and standardisation, which allows for seamless integration with other 5G technologies [14], [15].

Ned

C. NEED FOR THREAT LANDSCAPE IN 5G NETWORK FOR SRPS

Despite the security considerations incorporated into the 5G wireless access network design, several security flaws are associated with 5G technology.The following limitations are noteworthy [113], [114]:

1) Some of the newly introduced security features (including essential existing features) are defined as optional, or they present some degree of flexibility during the implementation interpretation of the controls. For instance, the use of confidentiality and integrity protection is optional for most access networks. This optional nature or flexibility in interpretation could introduce potential vulnerabilities, especially if the security control is poorly implemented.
2) Technical standards and specifications for security controls form the foundation for developing, implementing, and operating security controls. However, other essential factors, such as security testing and assurance, product development, network configuration and deployment, and network operation and management, are also crucial for successful and adequate security controls.
3) Security controls are more standardized for 3GPP access technologies as compared to non-3GPP access technologies. Most access network security controls depend on the availability of USIM, which securely stores secret keys; SRPS use cases may involve situations that do not require USIM to access the network. In some cases, the access technology may not be fully standardized to leverage the full security features introduced in 5G.
4) When a 5G access network operates in an NSA architecture, there is a strong possibility of a bidding-down attack, in which the network may drop certain security features available in 5G if a malicious actor deceives the network into believing that one end of the access network does not support these features. Although mitigation of bidding-down attacks is supported by 5G Release 18, this attack will be possible if some of the optional security features are not properly implemented.
5) The security assurances provided in 5G are based on use cases tested and investigated by various 3GPP working groups. As shown in Table 1, these results have undergone several revisions due to new findings and vulnerabilities. However, none of these use cases covers the unique SRPS scenarios.
6) The 5G access network will inherit the vulnerabilities of 4G and other heterogeneous technologies that are applicable to SRPS, such as network slicing, SDN, NFV, Restful API, and HTTPS.
7) Some of the human threat models in 5G may not work effectively for machine use cases like SRPS.
8) Integration of 3GPP access technology and non-3GPP access technologies, such as WiFi 6.

The security of 5G NSA is at risk from several LTE protocol exploits [70], [115], [116], [117], which include:

- Privacy threats, location leakage, and SS7 signalling vulnerabilities could lead to IMSI-catching attacks.
- Denial-of-Service (DoS) threats arising from Attach/Tracking Area Update (TAU) requests.
- Man-in-the-Middle (MITM) attacks that could enable calls and SMS snooping through the exploitation of the downgrade to GSM protocol.
- Inadequate protection for DNS traffic at layer 2.
- Location tracking using RNTI [71], [118].

To ensure the security of 5G NSA, it is important to implement measures that address these vulnerabilities and exploits.

IV. RELATED WORK

This section provides an overview of the existing literature on security threats to 5G networks. The studies discussed here address various aspects of 5G security, including the analysis of threat landscapes, vulnerability assessments, potential attack vectors, and proposed countermeasures.

A. THREAT LANDSCAPE AND VULNERABILITY ASSESSMENTS

Numerous studies have attempted to characterise the threat landscape in 5G networks. One such study by ENISA [8] identifies critical security threats and challenges in the 5G infrastructure, including the increased attack surface due to the integration of new technologies, the complexity of network management, and potential supply chain risks. The report also highlights the importance of network slicing and the need for enhanced security measures during actual implementation. However, this analysis is based on 3GPP standards and does not cover non-3GPP access networks or the specific challenges of SRPS.

Rao et al. [9] proposed a threat modelling framework called Bhadra for 5G mobile networks based on a review of academic publications and standards on mobile communication. The framework presents a general overview of mobile communication components while identifying potential threat actors. The authors categorise threats into nine tactical groups and identify 55 techniques. The Bhadra framework was evaluated using two case studies of mobile free mobile internet access and sim jacking attacks.

Similarly, Santos et al. [10] proposed the CONCORDIA Mobile Modelling Framework (CMTMF) for 5G mobile networks, incorporating inputs from MITRE'S ATT&CK and BHADRA frameworks. The framework identifies seven entry points to 5G Networks, and threats are addressed from two dimensions: mobile devices and virtualisation.

However, a drawback of these frameworks is that they were developed for mobile communication and 3GPP use cases and did not fully address the unique challenges of SRPS. Therefore, further research is needed to create comprehensive security frameworks that address the specific challenges of 5G networks, including SRPS.

B. ATTACK VECTORS AND KEY SECURITY CHALLENGES

Dutta and Hammad [11] provide an overview of 5G security challenges by examining 10 security pillars related to various enabling technologies, including network slicing security and supply chain security. The authors also present a threat taxonomy based on loss of security objectives and identify insider threats and service theft as potential security risks.

Tian et al. [12] surveyed publications from 2008 to 2016 on 5G C-RAN security and identified threats using the popular OSI model of physical, MAC, network, transport, and application layers. The authors discuss solutions to the security threats and vulnerabilities using the three planes. However, the study was conducted before the complete standardization of 5G, and the focus of the study was not on a specific use case.

Ahmad et al. [13] present an overview of 5G security challenges and solutions from five perspectives: key security challenges, SDN, NFV, MEC, and privacy challenges. The authors identify several threats to 5G security, such as hijacking, configuration attacks, saturation attacks, and user ID theft, and propose solutions from the reviewed literature. However, the study was conducted before the complete standardization of 5G security and did not address specific use case scenarios such as SRPS.

Ji et al. [130] provide a general overview of 5G security technology, highlighting its security requirements, architecture, and key technologies. The authors focus on the physical layer and network slice security, user privacy, and the need for blockchain technology in 5G security. Still, the study did not even focus on the RAN security of 5G.

Piqueras and Marojevic [115] analyze 5G specification protocol exploits with a focus on pre-authentication message-based exploits. The authors emphasize the need for a PKI-based architecture alternative to 5G to be completely standardized. Finally, the authors highlight all possible impacts of LTE vulnerabilities on 5G NSA.

Fang et al. [131] present 5G security services, enabling technologies, and architecture, with a focus on security solutions for IoT SDN use cases and not SRPS. The study was conducted at the beginning of standardization work in 5G networks.

In summary, the above-existing literature on 5G security highlights several key challenges, including the complexity of network management, the potential risks associated with the supply chain, and the need for enhanced security measures. However, many studies were conducted before the complete standardization of 5G security and did not address specific use case scenarios such as SRPS. Further research is needed to develop comprehensive security frameworks that address the unique challenges of 5G networks, including SRPS.

C. 5G MEC SECURITY

This subsection examines previous studies investigating 5G RAN with MEC potential from different perspectives, including security vulnerabilities [14], [15], [119], IoT integration [123], [124], [125], service migration [126], [127], computational offloading [128], and an interdisciplinary approach [110], [129]. However, none of these studies investigated SRPS as a use case for MEC using 5G RAN. The treatment of security threats was often too broad, with mMTC and cellular 5G communication dominating the discussion.

A recent study on SR threat landscape and attack surface in public spaces [2] identified four threat categories: cybersecurity, physical, social, and public space threats. The authors further classified cybersecurity threats into hardware, software, communication network, human (social engineering), cloud services, AI services, and supply chain threats. This study addresses both communication network and cloud services threats in their taxonomy, and our study is the first to investigate 5G RAN with MEC for SRPS.

Table 5 summarizes the research focus of some related works and their relevance to SRPS security threats. Although several studies have investigated 5G RAN with MEC potential, none have addressed the specific challenges of SRPS security threats. This highlights the need for further

TABLE 5. Related work on 5G RAN employing Multi-access Edge Computing (MEC).

Ref	Research focus	Relevance to SRPS security
[14]	conducted a comprehensive survey on the security and privacy of all 5G MEC systems, especially from a general 5G cellular communication perspective. The focus on MEC covered both core networks and services.	Although the study tried to address MEC systems, the emphasis was on mMTC and cellular communication. There was no focus on SR
[15]	The study focused on the security of 5G use cases such as autonomous vehicles (AV), unmanned aerial vehicles (UAV), and industrial robots	SR security use case was not covered
[119]	The paper focused on various CC paradigms and the proposed security solutions to identified threats	SR security use case was not covered. However, it discussed security in general.
[120]	Presented a survey on catching, computing, and communication techniques for MEC networks	Addressed general security issues on MEC networks, however, not related to SRPS
[121]	Presented a survey on communication and radio resource management from MEC computational perspective	Presented security and privacy with a focus on trust, and authentication, with no focus on SRPS
[122]	Presented a mobile virtual reality (VR) MEC use case deployment.	Did not cover MEC security and SRPS
[123]	Presented performance of IoT based on MEC deployment	Discussed the security and privacy of IoT using MEC. No discussion on SRPS
[124]	Presented MEC application potential in IoT deployment with consideration to mMTC use case	Discussed security in general MEC with no specifics to SRPS
[125]	Presented IoT use cases involving data analytics, computational offloading, surveillance and vehicle-to-infrastructure (V2I).	Did not address MEC security and SRPS use case
[126]	Presented service migration approaches of MEC	Proposed the use of blockchain for MEC security.
[127]	Presented virtual machine (VM) migration strategies in MEC	Discussed VM security but nothing on SRPS
[128]	Presented an end-to-end CC paradigm with a focus on offloading MEC, transparent computing and cloudlet	Discussed security and privacy in general with no focus on SRPS
[129]	Presented latency requirements of 5G with a focus on RAN.	MEC security and SRPS use case was not covered.
[110]	Presented a detailed survey on fog computing and related MEC paradigms	No specific focus on MEC security and SRPS

research to develop comprehensive security frameworks that address the unique challenges of SRPS in 5G networks.

V. SECURITY THREATS TO 5G NETWORKS FOR SRPS BASED ON SECURITY OBJECTIVES: CORE OBJECTIVES, THREATS, AND MITIGATIONS

In this section, we discuss the security threats to the 5G access network based on the core security objectives of SRPS. We begin by presenting and defining these objectives before moving on to discuss the threats and proposed mitigations, drawing from best practices and related works. Finally, Figure 5 provides an overview of the threats covered in this survey."

A. SECURITY OBJECTIVES FOR SRPS

The security objectives for SRPS can be categorized into four main areas: cybersecurity, physical security, social security, and public space security.

1) **Cybersecurity:** Cybersecurity objectives aim to protect SRPS from cyber-attacks and threats. This includes ensuring the confidentiality, integrity, availability, authentication, authorisation, and privacy of the robot's data, systems, and communication channels. Additionally, it involves protecting against software vulnerabilities, malware, and other cyber threats that could compromise the robot's functionality or expose sensitive information [132].
2) **Physical Security:** Physical security objectives aim to protect the SR from physical damage or unauthorized access. This includes ensuring the robot is physically secure from theft, vandalism, and other physical damage.
3) **Social Security:** Social security objectives aim to protect the SR from social threats, such as social engineering attacks or malicious behavior by individuals in public spaces. This includes ensuring that the robot's interactions with the public are appropriate, safe, and secure.
4) **Public Space Security:** Public space security objectives aim to ensure that the SR does not pose a threat to public safety or disrupt the normal functioning of public spaces. This includes ensuring that the robot's behaviour is safe and non-intrusive and that it does not cause any safety hazards or conflicts with other individuals in the public space.

The CIA triad definition of cybersecurity objectives by the National Institute for Standards and Technology (NIST FIPS 200) [133] is as follows: *"**confidentiality** entails preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. **Integrity** is guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity while availability is ensuring timely and reliable access to and use of information."*. The same NIST standard defines **authentication** as *"verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system."* Similarly, NIST SP 800-82 revision 2 [134] defines **authorization** as *"the right or a permission that is granted to a system entity to access a system resource"*. **Privacy** in the context of SR in public spaces can be defined as *"freedom from intrusion into the private life or affairs of an individual when that intrusion*

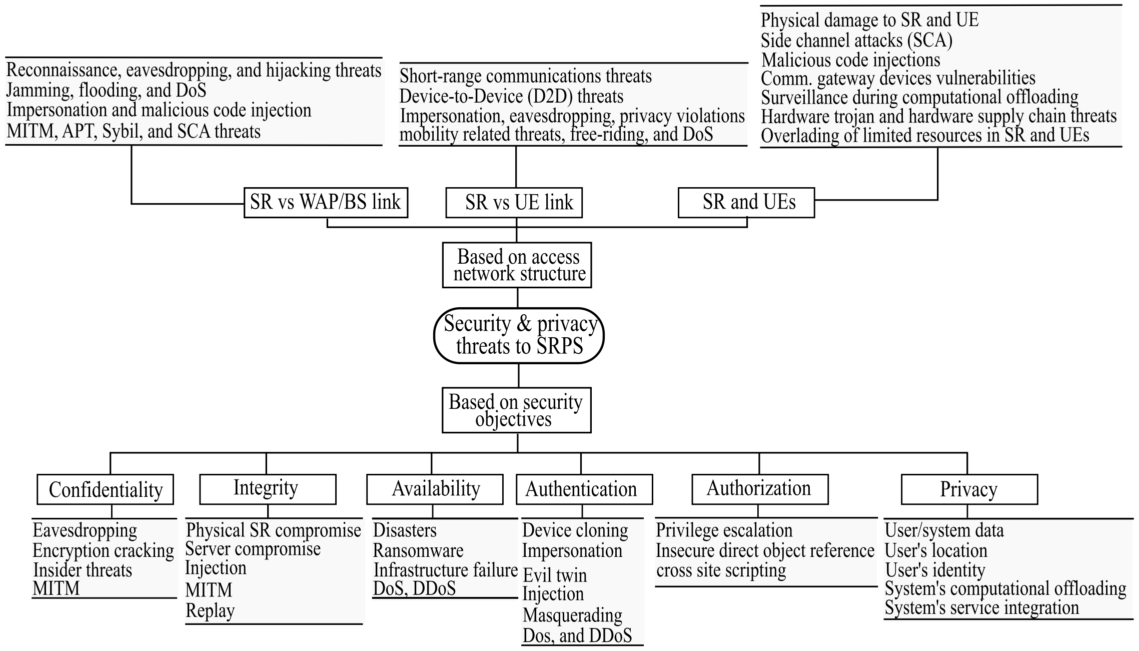
Reconnaissance, eavesdropping, and hijacking threats
Jamming, flooding, and DoS
Impersonation and malicious code injection
MITM, APT, Sybil, and SCA threats
Short-range communications threats
Device-to-Device (D2D) threats
Impersonation, eavesdropping, privacy violations
mobility related threats, free-riding, and DoS
Physical damage to SR and UE
Side channel attacks (SCA)
Malicious code injections
Comm. gateway devices vulnerabilities
Surveillance during computational offloading
Hardware trojan and hardware supply chain threats
Overlading of limited resources in SR and UEs
SR vs WAP/BS link
SR vs UE link
SR and UEs
Based on access network structure
Security & privacy threats to SRPS
Based on security objectives
Confidentiality
Integrity
Availability
Authentication
Authorization
Privacy
Eavesdropping
Encryption cracking
Insider threats
MITM
Physical SR compromise
Server compromise
Injection
MITM
Replay
Disasters
Ransomware
Infrastructure failure
DoS, DDoS
Device cloning
Impersonation
Evil twin
Injection
Masquerading
Dos, and DDoS
Privilege escalation
Insecure direct object reference
cross site scripting
User/system data
User's location
User's identity
System's computational offloading
System's service integration

FIGURE 5. Overview of threats discussed in this survey.

results from undue or illegal gathering and use of data about that individual." [135].

B. THREATS TO SRPS SECURITY OBJECTIVES

To ensure the safety and security of SR and their users in public spaces, it is important to address several threats to SRPS security objectives [2], including:

- **Cybersecurity Threats:** SRPS are vulnerable to cybersecurity threats, including hacking, malware, and denial-of-service (DoS) attacks. These attacks could compromise the robot's data and system security objectives. While the literature has extensively discussed cybersecurity threats to 5G networks, this subsection will later summarise cybersecurity threats relating to the SRPS use case.
- **Physical Threats:** Physical threats to SRPS include theft, vandalism, sabotage, and destruction, compromising the robot's functionality. Physical threats to 5G network infrastructure are also significant in this category. Generally, 5G network infrastructures are not given strict physical security like other information systems (e.g. server rooms and data centres). The functional split of the 5G fronthaul network increases the threat landscape, and a malicious physical attack on 5G infrastructures could cause significant damage.
- **Social Threats:** Social threats to SRPS include social engineering attacks, harassment, and malicious behaviour by individuals in public areas. These threats can compromise the robot's and its users' safety and security. SR ability to comply with social norms in public space is tightly connected to the 5G network QoS. Essential computational tasks, storage and AI services of SRPS will be carried out at the network's Edge (MEC). If the 5G network cannot support the required QoS due to failure or attack, social interactions will be seriously affected, resulting in human hostility or abuse of SR. It should be noted that social threats could also result from abnormal inputs (behaviours or responses) from humans that SR could not understand.
- **Public Space Threats:** Public space threats to SRPS include safety hazards, such as collisions with other objects or individuals and interference with the normal functioning of public spaces. As previously stated, the public space is dynamic and subject to many human/natural variables. These variables may affect the QoS of 5G networks, resulting in poor SR performance, while a hacked SR could threaten public space safety.
- **Supply Chain Threats:** Supply chain threats to SRPS include compromising hardware or software components during manufacturing, shipping, or installation, resulting in vulnerabilities or backdoors built into the robot's systems. In addition, with the introduction of O-RAN in 5G networks, where diversity and interoperability are encouraged among RAN vendors, supply chain threats are becoming a significant concern not yet standardised by the 3GPP. With the introduction of PKI to manage trust relationships in 5G networks, there is a need to standardise and create certifications for PKI service providers (CAs). With the proliferation of open-source software, AI models, and third-party applications that SRPS will rely on, supply chain threat is a significant concern for SRPS.

- **Privacy Threats:** SRPS may collect and process sensitive user data, such as images and voice recordings. Privacy threats include this data's unauthorised collection, use, or disclosure, compromising users' privacy and security. While the literature has covered privacy threats, this subsection will later summarise these privacy-related threats for SRPS for completeness.

While each of these threats poses a significant risk to the security objectives of SRPS, they can be addressed through appropriate security measures and protocols.

1) CYBERSECURITY THREATS

Practitioners and researchers developing an SRPS use case that utilizes 5G networks should be aware of potential cybersecurity threats that could compromise confidentiality, integrity, availability, authentication, and authorization. While the proper implementation of 5G security standards as specified by 3GPP SA 3 [46] can address most of these issues, any flaws in the use case implementation can expose it to the following potential threats. Therefore, it is essential for responsible IT practitioners to be vigilant and take the necessary steps to mitigate these threats.

a: CONFIDENTIALITY THREATS

The cybersecurity threats [130] to our use case's *confidentiality* include

- **Eavesdropping:** Attackers can intercept communication between two devices, potentially allowing them to access sensitive information.
- **Man-in-the-middle (MITM) attacks:** In a MITM attack, an attacker intercepts communication between two parties, potentially allowing them to alter or steal information.
- **Encryption cracking:** Attackers can attempt to decrypt encrypted information, potentially allowing them to gain access to sensitive information.
- **Insider threats:** A trusted individual with access to the system could intentionally or unintentionally cause harm to the system or data. For example, an employee with access to the 5G network's control system could deliberately or accidentally alter or delete critical data.
- **Malware:** Malicious software can compromise the confidentiality of 5G networks, including keyloggers, trojans, and ransomware.
- **Rogue devices:** Unauthorized devices can access the 5G network, potentially compromising the confidentiality of the network.
- **Interception of radio signals:** Attackers can intercept and analyse radio signals transmitted by the 5G network, potentially allowing them to access sensitive information.

b: INTEGRITY THREATS

Threats to the *integrity* of 5G networks can include attacks that aim to modify, delete, or disrupt the data or functionality of the network components. Some examples of such threats are:

- **Man-in-the-middle (MITM) attacks** intercept the communication between two devices and modify the transmitted data without the users' knowledge. MITM attacks can compromise the integrity of 5G networks by changing or deleting the data packets or injecting malicious content.
- **Replay attacks** involve the interception and retransmission of valid data packets to gain unauthorised access or disrupt the network. Replay attacks can compromise the integrity of 5G networks by causing the network to process the same data twice or more, leading to unexpected results or system failure.
- **Injection attacks** involve the injection of malicious code or data into the network to modify the system's behaviour or steal sensitive information. Injection attacks can compromise the integrity of 5G networks by changing the data packets, exploiting vulnerabilities in the software, or gaining unauthorised access to the network.
- **Physical compromise:** Physical compromise of network components can also compromise the integrity of 5G networks, resulting in unauthorised access, modification or destruction of the system. Physical attacks can include theft, vandalism, sabotage, and destruction of network infrastructure.
- **Server compromise:** Compromise of network servers can result in the unauthorised access, modification, or deletion of data. Attackers can exploit vulnerabilities in the software or hardware of the servers or gain unauthorised access through weak passwords or unsecured access points. Server compromise can also lead to DoS attacks that can disrupt the availability of the network.

c: AVAILABILITY THREATS

There are several threats to *availability* in 5G networks, including:

- **Natural disasters:** Natural disasters such as floods, earthquakes, hurricanes, and tornadoes can cause damage to 5G network infrastructure, disrupting the availability of the network.
- **Infrastructure failure:** Equipment failure, network congestion, and power outages can all cause disruptions to 5G network availability.
- **Cyberattacks:** Denial-of-service (DoS) attacks can overwhelm the 5G network with traffic, causing disruptions to availability.
- **Ransomware attacks:** Ransomware can encrypt critical files and demand payment to restore them, potentially causing disruptions to the availability of the 5G network.
- **Network misconfiguration:** Misconfigured network settings can cause disruptions to the availability of the 5G network.
- **Human error:** Human errors, such as misconfiguration of network settings or accidental damage to network

infrastructure, can cause disruptions to the availability of the 5G network.

- **Supply chain issues:** Issues in the supply chain, such as a shortage of equipment or delays in delivery, can cause disruptions to the availability of the 5G network.

d: AUTHENTICATION THREATS

Threats to *authentication* of 5G networks include:

- **Device cloning:** Attackers can clone a legitimate device's International Mobile Equipment Identity (IMEI) number and make it appear as a trusted device.
- **Masquerading attacks:** Attackers can impersonate a legitimate device or user to gain access to the network.
- **Evil twin attacks:** Attackers can set up fake access points (APs) that are legitimate to trick users into connecting to them.
- **Denial of Service (DoS) attacks:** Attackers can flood the network with traffic, making it difficult or impossible for legitimate users to access.
- **Injection:** Attackers can inject malicious code into legitimate network traffic to gain unauthorised access to the network.
- **Distributed Denial of Service (DDoS) attacks:** Attackers can use a botnet to launch a coordinated attack on the network, overwhelming it with traffic and making it unavailable to legitimate users.

e: AUTHORISATION THREAT

Threats to *authorisation* in 5G networks can include:

- **Privilege escalation:** Attackers may exploit vulnerabilities in the network to elevate their privileges, granting them access to unauthorised resources or systems.
- **Cross-site scripting (XSS):** Attackers inject malicious code into a web application, which is then executed by users who access the application. This can lead to unauthorised access to sensitive data or systems.
- **Insecure direct object reference:** Attackers exploit vulnerabilities in the network to access or manipulate objects, such as files or databases, that they are not authorised to access.

2) PRIVACY THREATS

The threats to the *privacy* of 5G networks can be classified into several categories, including:

- **User/System Data:** This includes the unauthorised collection, use, or disclosure of sensitive user data such as personal information, browsing history, and communication content.
- **User Location:** This involves tracking and monitoring user location without their consent or knowledge, which can lead to privacy violations.
- **User Identity:** This involves the unauthorised use or disclosure of user identity information, which can be used for malicious purposes like identity theft.
- **System Usage Profiling:** This involves the unauthorised monitoring and profiling of users' behaviour and preferences, which can compromise their privacy.
- **Computational Offloading** involves transferring data and processing tasks to third-party service providers, which can lead to privacy violations if the sensitive data is not adequately protected.
- **Service Integration:** This involves integrating different services and applications, which can lead to privacy breaches if the integration is not adequately secured.

Ensuring user privacy is a major concern in the use case of SRPS, with regulatory statutes such as GDPR providing guidelines to this effect. As per Ranaweera et al., [14], privacy threats can be classified into six categories: (i) user/system data, (ii) user location, (iii) user identity, (iv) system usage profiling, (v) computational offloading, and (vi) service integration. Similarly, Kumar et al. [136] identified three privacy dimensions: user, data, and services, with location and identity being part of user privacy and data privacy involving the sharing of such data between network communication infrastructures. The sensitive user data collected by SRPS will be transferred between various MEC infrastructure operators, including service providers, third-party services, and mobile network operators, making it difficult to guarantee the privacy of such data. Malicious users can track other users' location data, while hackers could access identity information used by SRPS, resulting in privacy violations. A malicious user monitoring the system data for SR can build a usage profile for such a system, thereby violating its users' privacy. Privacy violation issues may also result from monitoring system logs relating to computational offloading and service migration of SRPS.

C. MITIGATIONS OF SRPS THREATS BASED ON SECURITY OBJECTIVES

The 3GPP security standard, as specified in TS33.501 [46], provides a comprehensive set of guidelines for ensuring the security of 5G networks, covering most of the security concerns discussed in this section. However, it does not explicitly address physical, supply chain, and public space threats, critical concerns for SRPS. In scenarios where the Non-Standalone Architecture of the 5G network is utilised for SRPS, it is essential to implement additional measures to address these threats. Although few studies have investigated security issues related to SRPS in public spaces, some best practices and standards can influence mitigation strategies. Below are some suggested mitigations: (i) *Physical threats:* Secure the physical infrastructure and assets that support the SRPS use case, such as the robots, network nodes, and other hardware components. Implement access controls, surveillance systems, and other physical security measures to prevent theft, vandalism, sabotage, and other forms of physical compromise. (ii) *Supply chain threats:* Verify the integrity of the hardware and software components used in the SRPS use case, especially during manufacturing, shipping, and installation. Implement secure boot and firmware update mechanisms and supply chain risk management practices to prevent the compromise of the robot's systems. (iii) *Public space threats:* Collaborate with relevant stakeholders, such as city authorities, law enforcement agencies, and the public, to mitigate the risks associated with public space threats. Implement safety and emergency response protocols, such as collision detection and avoidance, and ensure that the robots comply with their public spaces' social norms and regulations. The above measures are not exhaustive and should be customised to the specific SRPS use case and operational environment. Additionally, the responsible IT team should continuously monitor the security posture of the SRPS use case and update the mitigation strategies as necessary. Specific mitigations for each identified threat are presented below.

1) CYBERSECURITY THREATS MITIGATIONS

The following section discusses mitigation strategies for various cybersecurity threats, including confidentiality, integrity, availability, authentication, authorisation, and privacy.

a: CONFIDENTIALITY THREATS

Several mitigations against *confidentiality threats* to 5G networks are already covered by 3GPP 5G security features if properly implemented. including:

- **Encryption:** The use of encryption algorithms, such as AES and RSA, can help protect data confidentiality by encrypting the data in transit and at rest.
- **Key management:** Proper key management practices, such as secure key storage and distribution, can prevent unauthorized access to encryption keys.
- **Access control:** Access control mechanisms, such as firewalls, intrusion detection and prevention systems, and network segmentation, can limit access to sensitive data and prevent unauthorized access.
- **Network security monitoring:** Network security monitoring tools can detect and alert suspicious network activity that may indicate a confidentiality breach.
- **Security awareness training:** Providing security awareness training to employees and users can help prevent unintentional disclosure of sensitive information.
- **Regular vulnerability assessments:** Regular vulnerability assessments can help identify and mitigate potential vulnerabilities that may lead to confidentiality breaches.
- **Proper handling of sensitive data:** Implementing policies and procedures for the proper handling of sensitive data can help prevent unintentional or unauthorized disclosure of the data.
- **Use of secure communication protocols:** Using secure communication protocols, such as SSL/TLS and SSH, can help ensure the confidentiality of data in transit.

There are several other proposed solutions to address threats to confidentiality in 5G networks. One approach is to use lightweight encryption methods, such as elliptic curve cryptography [137] or post-quantum cryptographic solutions [16]. Another option is to implement end-to-end (E2E) security using IP security (IPSec) or transport layer security (TLS) encryption [119]. These solutions can help ensure that confidential data is protected and not accessible to unauthorised parties.

b: INTEGRITY THREATS MITIGATIONS

The following are mitigations against *integrity threats* to 5G networks, including:

- **Encryption:** Encryption is one of the most effective ways to protect against integrity threats. Encrypting data in transit and at rest makes it much harder for attackers to modify or tamper with the data.
- **Secure protocols:** Using secure protocols for communication, such as HTTPS and TLS, can help prevent man-in-the-middle attacks and ensure that data remains intact during transit.
- **Network segmentation:** Segmentation of the network into smaller, more manageable segments can help prevent attacks from spreading throughout the entire network.
- **Access controls:** Implementing strong access controls, such as two-factor authentication and access policies, can help prevent unauthorized access and modification of data.
- **Intrusion detection and prevention:** Using intrusion detection and prevention systems (IDPS) can help detect and prevent attacks on the network, thereby preventing data tampering and modification.
- **Regular audits:** Regular audits and assessments of the network can help identify vulnerabilities and weaknesses that attackers can exploit. This can help organizations proactively address potential threats to network integrity. Overall, a multi-layered approach to security is necessary to mitigate integrity threats to 5G networks effectively.

5G authentication and key agreement (AKA) standards [138] can prevent threats to the integrity of 5G networks.

c: AVAILABILITY THREATS MITIGATIONS

Several mitigations can be implemented to address availability threats to 5G networks. Some examples are:

- **Redundancy:** Redundancy can be implemented at various levels of the network to ensure that if one component fails, there is another to take over its function. Redundancy can be implemented for both hardware and software components.
- **Disaster recovery:** A disaster recovery plan can be put in place to ensure that the network can quickly recover from natural disasters, such as earthquakes or floods, and man-made disasters, such as cyber-attacks.
- **DDoS mitigation:** Distributed denial of service (DDoS) attacks can be mitigated by using rate limiting, IP blocking, or traffic filtering techniques.
- **Network segmentation:** Network segmentation can be implemented to ensure that if one segment of the network is compromised, the rest of the network remains operational.

- **Access control:** Access control mechanisms can be implemented to ensure that only authorized personnel have access to critical components of the network.
- **Patch management:** Regular patching of software components can address vulnerabilities that attackers could exploit to compromise network availability.
- **Capacity planning:** Capacity planning can ensure that the network has sufficient capacity to handle the expected traffic and can scale up or down as needed.

In addition, we can ensure the availability of MEC-enabled networks by placing SR applications at the MEC edge host [139], adopting tenant isolation in a multi-slice environment [140], providing hash-based and session-based encryption schemes [141], and using the encapsulation security payload attribute of IPSec [142].

d: AUTHENTICATION THREATS MITIGATIONS

To mitigate authentication threats to 5G networks, the following measures can be implemented:

- **Use of strong authentication mechanisms:** To mitigate the threat of device cloning and impersonation attacks, strong authentication mechanisms such as biometric authentication, two-factor authentication, and multi-factor authentication can be used.
- **Implementation of secure communication protocols:** Implementing secure communication protocols such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL) can prevent man-in-the-middle (MITM) attacks and injection attacks.
- **Implementation of intrusion detection systems:** Intrusion detection systems (IDS) can be deployed to detect and prevent denial of service (DoS) and distributed denial of service (DDoS) attacks.
- **Continuous monitoring and logging:** Continuous monitoring and logging of network activities can help detect and respond to any unauthorized access attempts or suspicious activities.
- **Implementation of strong access control policies:** Access control policies can be implemented to restrict access to sensitive network resources and prevent privilege escalation attacks.
- **Regular security audits and updates:** Regular security audits and updates can help identify and fix any vulnerabilities or weaknesses in the network's authentication mechanisms.

Various authentication schemes have been proposed to prevent authentication threats, including post-quantum cryptography [16], Bluetooth low energy (BLE) [143], radio frequency identification (RFID) [144], Narrow-band IoT (NB-IoT) [145], Light Fidelity (LiFi) data [146], physical unclonable function (PUF) [147], and accelerometer data [148].

e: AUTHORISATION THREATS MITIGATION

There are several mitigations against **authorization threats** to 5G networks, including

- **Role-based access control (RBAC):** RBAC limits access to resources based on the user's role and responsibilities. This reduces the risk of unauthorized access to sensitive data or systems.
- **Attribute-based access control (ABAC):** ABAC restricts access to resources based on the user's attributes, such as job title, location, or security clearance. This provides more granular control over access than RBAC.
- **Regular security audits:** Regular security audits help identify and address authorisation system vulnerabilities.
- **Multi-factor authentication (MFA):** MFA requires users to provide two or more forms of authentication, such as a password and a fingerprint scan, before accessing sensitive data or systems. This makes it more difficult for attackers to gain unauthorized access.
- **Principle of least privilege:** This principle limits access to resources to the minimum level required to perform a user's job function. This reduces the risk of accidental or intentional misuse of data or systems.
- **Security information and event management (SIEM):** SIEM systems collect and analyze security-related data from various sources to detect and respond to security incidents in real-time.
- **Secure coding practices:** Secure coding practices can help prevent authorization vulnerabilities, such as SQL injection attacks and cross-site scripting (XSS) attacks, by ensuring that code is written securely.

Some proposed ways of mitigating authorisation threats in MEC include using security log monitoring [149], adopting a trusted platform manager (TPM) [150], adopting blockchain technology [151], and using 5G extensible authentication protocol (EAP) AKA [131].

f: PRIVACY THREATS MITIGATIONS

To address privacy threats in 5G networks, several mitigations can be implemented, including:

- **Encryption:** Implementing end-to-end encryption to protect user data and prevent eavesdropping and interception of sensitive information.
- **Access control:** Implementing access control mechanisms such as firewalls, intrusion detection and prevention systems (IDPS), and identity and access management (IAM) solutions to prevent unauthorized access to sensitive data.
- **Anonymization:** Anonymizing user data to protect their identity and location information.
- **Data minimization:** Limiting the collection and storage of sensitive user data to only what is necessary to provide the service and implementing policies for secure data disposal.
- **Transparency:** Providing users with clear and concise information about how their data is collected, used, and shared allows them to control their preferences.

- **Privacy by design:** Implementing privacy considerations into developing new 5G technologies and applications, including data protection impact assessments (DPIA).
- **Compliance with regulations:** Ensuring compliance with privacy regulations such as GDPR, CCPA, and other relevant laws and standards.

Jiang et al. [152] summarised the mitigations for location privacy-preserving mechanisms as privacy policy [153], obfuscation, cryptography, and cooperation/caching approaches. Examples of obfuscation include cloaking, dummy locations, differential privacy, mix zones, and path confusion, while space transformation, secure multi-party computation (SMC) [154], and private information retrieval (PIR) [155] are proposed cryptographic approaches. Gai et al. [156] suggested using a permissioned blockchain solution to preserve the privacy of smart grid networks. He et al. [157] employed a chaff-based approach to confuse eavesdroppers as a location privacy preservation measure. It is important to note that implementing multiple mitigation techniques in combination is necessary to provide a comprehensive approach to privacy protection in 5G networks.

2) PHYSICAL THREAT MITIGATIONS

There are several mitigations against physical threats to 5G networks, including:

- **Physical security measures:** This includes measures such as security cameras, alarms, access controls, and security personnel to secure the physical infrastructure of the 5G network.
- **Hardening of network components:** This involves hardening the physical infrastructure of the 5G network, including base stations, routers, and switches, to make them more resistant to physical attacks.
- **Backup and redundancy:** This involve having backup and redundant systems in place to ensure continuity of service in the event of physical damage or failure.
- **Disaster recovery and business continuity planning:** This involves developing plans and procedures to ensure the 5G network can quickly recover from physical disasters and continue providing service.
- **Supply chain security:** This involves ensuring the security of the supply chain for network components, including verifying the authenticity and integrity of hardware and software components.
- **Regular security assessments:** Regular security assessments can help identify vulnerabilities and weaknesses in the physical security of the 5G network and help to develop appropriate mitigations.

3) SUPPLY CHAIN THREATS

There are several mitigations against supply chain threats to 5G networks, including:

- **Vendor and supplier security assessments:** 5G network operators can carry out comprehensive security assessments of their vendors and suppliers to ensure adequate security controls are in place to protect against supply chain threats.
- **Secure software development practices:** 5G network operators can ensure that their vendors and suppliers follow secure software development practices, such as using secure coding techniques and performing vulnerability assessments and penetration testing.
- **Encryption and authentication:** 5G network operators can use encryption and authentication mechanisms to protect against supply chain attacks that compromise network traffic's confidentiality and integrity.
- **Network segmentation and access controls:** 5G network operators can implement network segmentation and access controls to limit the impact of supply chain attacks that compromise individual network components.
- **Regular security assessments:** 5G network operators should conduct regular security assessments to identify and mitigate any vulnerabilities or weaknesses in the supply chain.
- **Trust and certification of components:** 5G network operators can ensure the trust and certification of all components used in the network by requiring suppliers to meet specific security standards and obtaining certificates from trusted third-party organisations.
- **Continuous monitoring and threat intelligence:** 5G network operators can implement continuous monitoring and threat intelligence capabilities to detect and respond to supply chain threats in real time.

4) PUBLIC SPACE THREATS MITIGATIONS

Public space threats to 5G networks, such as collisions and interference, are typically mitigated through physical measures, such as the placement of barriers or warning signs. In the case of SRPS, additional measures such as creating designated areas for the robots and restricting their movement to certain times of the day or specific routes can also be implemented. Using sensors and cameras in the environment can provide real-time monitoring and detection of potential threats to public space safety. Additionally, regular maintenance and inspection of the robot and its surrounding environment can identify and address potential hazards before they become a problem. A multi-layered approach to physical security that combines hardware, software, and operational procedures can help mitigate public space threats to 5G networks.

Table 6 presents a summary of the security threats and proposed mitigations based on security objectives of confidentiality, integrity, availability, authentication, authorization, and privacy for SRPS.

VI. SECURITY THREATS AND MITIGATIONS TO 5G NETWORKS FOR SRPS BASED ON NETWORK STRUCTURE

The 5G radio access network (RAN) comprises various heterogeneous technologies as specified by 3GPP [162]. The heterogeneous technologies in 5G networks include:

TABLE 6. Summary of security threats and proposed mitigations based on security objectives for SRPS.

Security objectives	Threats	Mitigations
Confidentiality	Eavesdropping Man-in-the-middle (MITM) Encryption cracking Insider threat	(i) Post-quantum cryptographic solutions [16] (ii) E2E security using IPSec or TLS/SSL tunnelling [119] (iii) Light-weight security protocol [137]
Integrity	Physical SR compromise MITM, Replay, Injection Server compromise	Using 5G Authentication and Key Agreement (AKA) [138]
Availability	Denial-of-Service (DoS) Disasters Ransomware Infrastructure failure	(i) Effective placement of SR apps in the mobile edge host of the MEC [139]. (ii) Adopting tenant isolation in a multislice environment [140], (iii) Using hash-based and session-based encryption schemes [141], and (iv) Using encapsulation security payload attribute of IPSec [142]
Authentication	Device cloning Masquerading attacks Impersonation Evil twin Injection DoS and DDoS	Using suitable authentication such as (i) post-quantum crypto [16] (ii) BLE [143], (iii) RFID [144] (iv) NB-IoT [145], (v) LiFi data [146] (vi) PUF [147], and (vii) accelerometer data [148].
Authorization	Privilege escalation Insecure direct object reference Cross-site scripting	(i) Security log monitoring [149] (ii) use of blockchain technology [151] (iii) 5G EAP AKA [131] (iv) TPM [150]
Privacy	User/system data User's location User's identity Usage profiling System's computational offloading, System's service integration	(i) privacy policy [153], (ii) Obfuscation (e.g. cloaking) [158] (iii) cryptography [153], (iv) blockchain [156], (v) chaff services [157]. (vi) computational offloading [159], (vii) privacy partitioning [160] (viii) privacy-preserving model [161]

1) **Worldwide Interoperability for Microwave Access (WiMAX):** a wireless broadband technology that operates on a range of frequencies and can provide high-speed Internet access.
2) **Orthogonal Frequency Division Multiple Access (OFDMA) networks:** a multi-user version of the popular Orthogonal Frequency Division Multiplexing (OFDM) digital modulation scheme for wideband digital communication.
3) **Wireless Local Area Network (WLAN):** a wireless networking technology that uses radio waves to provide high-speed Internet and network connections over short distances. The most suitable option for SRPS is Wi-Fi 6. Wi-Fi 6 is the sixth generation of Wi-Fi technology, also known as 802.11ax. It is the successor to Wi-Fi 5 (802.11ac) and offers several improvements in terms of speed, capacity, and efficiency. Wi-Fi 6 is designed to provide faster and more reliable connectivity in environments with many connected devices, such as crowded public spaces, offices, and homes. Some of the key features of Wi-Fi 6 include higher data rates, increased network capacity, improved performance in dense environments, and better power efficiency. It also includes technologies such as MU-MIMO, OFDMA, and 1024-QAM, allowing for more simultaneous connections and greater throughput.
4) **Satellite communication:** a communication technology that uses artificial satellites to provide communication links between various points on Earth. In sensitive SRPS use cases, satellite communication could provide redundancy and ensure reliability in SRPS 5G networks.
5) **Microwave links:** a point-to-point communication technology that uses high-frequency radio waves to transmit data between two locations.
6) **Millimeter-wave (mmWave):** a high-frequency radio wave technology that can transmit large amounts of data over short distances.
7) **Small cells:** a network technology that uses small, low-power cellular base stations to provide improved coverage and capacity in densely populated areas.
8) **HetNet (Heterogeneous Network):** a network architecture that combines different wireless technologies, such as 3G, 4G, and Wi-Fi, to improve coverage, capacity, and quality of service.

Due to the diverse and heterogeneous nature of these enabling technologies, the RAN of 5G is an attractive target for many threat actors [12].

In this section, we classify the threats to SR WAN into three groups, based on insights from Ranaweera et al. [14]: (i) threats between SR and wireless access points (or base station), (ii) threats between SR and user devices (such as phones), and (iii) threats to SR and user devices.

A. THREAT TO SRPS BASED ON ACCESS NETWORK STRUCTURE

The 5G access network for SRPS is vulnerable to various threats, including physical, roaming, DDoS, and virtualisation (containerisation) threats. **Physical threats** to 5G networks refer to threats that arise from unauthorised physical access to network infrastructure. These threats include *vandalism*, such as physical damage to 5G network infrastructure like antennas, base stations, and other network equipment; *theft* of network infrastructure, such as radios and antennas, which can disrupt network operations and compromise network security; *environmental hazards*, like natural disasters such as earthquakes, floods, and storms, that can damage 5G network infrastructure and disrupt network operations; *power outages*, which can cause disruptions in network operations and create opportunities for attackers to exploit vulnerabilities, and access control breaches, such as unauthorised physical access to network equipment that can allow attackers to compromise network security. The fronthaul of the 5G network is particularly vulnerable to security breaches because it is easily accessible and lacks adequate physical security, such as data centres or enterprise control/server rooms. Malicious attackers can easily break into the cabinets of 5G networks to access switches, routers, and compute modules. Attackers can insert pen drives into the ports of these modules and corrupt system software applications. Physical security measures, such as access control systems, surveillance cameras, and alarms, are crucial to protect 5G network infrastructure from physical threats.

Roaming threats to 5G networks pose security risks when users move from their home network to a visited network while maintaining connectivity. These threats can include unauthorized access, network breaches, and interception of data by malicious actors. Roaming threats can be aggravated when using unsecured or untrusted networks, such as public Wi-Fi hotspots or unencrypted networks. Attackers can exploit vulnerabilities in the roaming connection to launch various types of attacks, including man-in-the-middle attacks and eavesdropping. Roaming threats are particularly significant because they grant attackers direct access to the 5G network core. 5G networks are known to have several signalling vulnerabilities and inadequate controls, which make them susceptible to roaming threats.

The wireless communication link between SRPS and their corresponding wireless access point (WAP) or base station utilises several enabling technologies such as millimetre wave (mmWave), beamforming, and WiFi offloading to meet high data rate and low latency requirements [163]. This wireless link is susceptible to three groups of threats: (a) reconnaissance, eavesdropping, and hijacking threats, (b) jamming, flooding, and denial of service (DoS) attacks, and (c) impersonation and malicious node injection threats. Malicious actors attempt various attacks such as man-in-the-middle (MITM) attacks, Sybil attacks, and spoofing attacks to understand SR operations, eavesdrop, or hijack communications. Flooding sensors with too many signals, jamming, and other forms of DoS attacks are also possible at this level of communication. Cybercriminals may impersonate a legitimate node or inject a malicious node within the vicinity of the SR, compromising the communication link.

The ad hoc link between SR and users' devices is vulnerable to short-range communication and device-to-device (D2D) threats. This link employs heterogeneous enabling technologies such as Bluetooth Low Energy (BLE), Near Field Communication (NFC), WiFi, ZigBee, NB-IoT, SigFox, Bluetooth 4.0, and Mobile Ad hoc Networks (MANET) [164]. Security threats to this communication link include impersonation, eavesdropping, privacy violations, mobility threats, free-riding, and DoS attacks [165]. Attackers may attempt to impersonate a legitimate device to gain access to sensitive information or to carry out malicious actions. Eavesdropping is also a concern, as attackers can intercept and access the communication between SR and users' devices. Privacy violations can occur if attackers access personal data, compromising users' privacy. Mobility threats include location tracking, where attackers can track the location of SR and users' devices. Free-riding attacks occur when an attacker uses the resources of other devices in the network without contributing to the network's operation. Finally, DoS attacks can disrupt the communication between SR and users' devices, leading to service outages.

The final group of threats targets the SR and user devices (UE) used during social interactions. This group includes smartphones, wearables, cameras, smartwatches, and other devices with different operating systems, such as Android, iOS, Windows, Symbian, Blackberry, and WebOS. They use various communication protocols such as RFID, NFC, BLE, and WiFi, all vulnerable to attacks. These devices contain personally identifiable information (PII), such as users' account information, medical records, location information, daily preferences and routine information, and critical infrastructure information for those responsible for monitoring and maintenance. However, they are resource-constrained in computation, processing, battery, and storage capacity, increasing their vulnerability.

The following are some of the threats affecting SR and user devices that are in communication with them:

- Physical damage to SR and user devices can include device reconfiguration, resulting in a node sending misleading or wrong information.
- Surveillance threats during computational offloading of SR and user equipment.
- Side-channel attacks (SCA) that eavesdrop on communication patterns or crack the cryptographic algorithms that these communicating nodes use.
- Malicious code injection threats resulting from malware, viruses, ransomware, adware, spyware, rootkit, worms, or Trojan attacks.
- Communication gateway device vulnerabilities that malicious actors can exploit, such as directing attacks at access points, SC, etc., within the communication link.
- Hardware Trojan threats that could result from hardware supply chain vendors.
- Threats from overloading the limited resources of SR and users' equipment.

TABLE 7. Proposed solutions to social robot access network threats.

Threat to	Proposed solutions	Reported in
Social Robot vs Wireless Access Points network	Adopting 5G wireless security architecture	[131]
	Physical layer security	[166]
	Using AES 256-bit encryption and secure signalling	[167]
	Using RT channel model for 5G mmWave in SC	[168]
Social Robot vs User Equipment network	PUF schemes based on 2FA for UEs	[137]
	PUF schemes based on FPGA (TERO)	[145]
	Adopting a layered security deployment	[165]
	Autonomous authentication schemes for D2D	[146]
	Authentications schemes based on IBE PHY-ID	[169]
Social Robot & User Equipment	Security and privacy-enhancing framework	[170]
	Automatic detection of SCA attacks using ML	[171]

B. MITIGATIONS TO SRPS THREATS BASED ON ACCESS NETWORK STRUCTURE

Implementing 5G security architecture and standards specified by 3GPP SA 3 can mitigate most identified threats based on access network structure. However, special precautions should be taken in 5G non-standalone architecture cases and other non-3GPP access networks.

To mitigate physical threats to 5G networks, security measures such as access controls, video surveillance, and physical security monitoring should be implemented. Regular equipment inspections and maintenance can also help identify and address physical vulnerabilities. Additionally, backup power supplies, redundant network connections, and disaster recovery plans can help ensure network availability during power outages or other environmental hazards. Additional implementation of endpoint security and network access control consisting of port security, dynamic ARP inspections, and trusted hardware security could further help harden protection against physical access attacks. The adoption of zero-trust principles through public key infrastructure (PKI) and IPSec tunnelling, especially when third-party lease lines exist between access points and network edge.

Anti-DoS and throttling can be used to mitigate DDoS attacks. Anti-DoS measures include rate limiting, traffic filtering, and IP blocking to prevent malicious traffic from overwhelming the network or server. In 5G networks, anti-DDoS techniques may also involve using machine learning algorithms to detect and mitigate attacks in real time and leveraging the network's distributed architecture to distribute traffic and avoid single points of failure. Throttling is a network management technique used to regulate the data traffic on a network. In 5G security, throttling can be used as a security measure to prevent DoS attacks and other types of malicious traffic from overwhelming the network.

Various proposed solutions have been suggested to address the threats to 5G RAN networks. These solutions aim to ensure the security and privacy of the network infrastructure and the SRPS.

One proposed solution is encryption [167], which involves end-to-end encryption to protect user data and prevent eavesdropping and interception of sensitive information. Another solution is implementing physical layer security [166], which consists in securing the physical network infrastructure to prevent unauthorised access and interference.

Other solutions include security architectures [131], which provide a framework for implementing security measures in the network, 5G ray tracing-based mmWave channel models [168], which model and simulate radio wave propagation to optimise the network performance, lightweight cryptography [172], which uses efficient and low-complexity cryptographic algorithms to minimise the impact on network performance, and post-quantum cryptography [173], which involves using cryptographic algorithms that are resistant to quantum computing attacks.

Autonomous authentication [167], and PUF [165], [169], [174], [175] are also proposed solutions to mitigate authentication threats. These methods involve using unique physical properties of devices to verify their identity and ensure secure communication.

Other proposed solutions include 2-factor authentication [176], layered security architecture [165], and side channel attack detection [171], [177], [178]. 2-factor authentication involves requiring users to provide two forms of authentication before accessing sensitive data or systems. In contrast, layered security architecture involves implementing multiple security measures to prevent attacks. Side channel attack detection involves detecting and mitigating attacks that exploit vulnerabilities in implementing cryptographic algorithms.

Table 7 summarises some proposed solutions to the access networks of SRPS, highlighting their benefits and limitations. These solutions can be combined to create a comprehensive security framework for SRPS.

C. CENTRALIZED LEDGER DATABASES: HARNESSING ADVANCES FOR STRENGTHENED DATA SECURITY

A centralised ledger database operates under a central authority that manages and controls all the data. Without consensus, one entity or organisation controls all operations, including data reading, writing, and modification. The central entity is also responsible for security and backups. Fekete and Kiss [184] deliver an exhaustive exploration of the applications of ledger databases within conventional database management. Their study divides ledger databases into two

TABLE 8. Comparative Analysis of centralised and decentralised Ledger Solutions: Database Type, Platform, and Performance Perspectives.

Solution	DB Type	Cloud Platform	Pros	Cons
LedgerDB [179]	Centralised	Alibaba	High throughput, Low latency, Strong auditability, Ease of use	Verification costs can be high
GlassDB [180]	Both	Not available	High performance, Verifiability, Efficient protection of indexes	Emphasis is on audit verifiability and read/write transactions
SQL Ledger [181]	Centralised	Azure SQL Server	Cryptographic data integrity, Power and flexibility of a commercial RDBMS	Lower throughput and verifiability
TABI [182]	Decentralised	Hyperledger	End-to-end security in IoT networks, Mitigates malicious user impact	The decentralised nature may affect its suitability for SRPS
PReVer [183]	Both	Not available	Consistent and verifiable update execution, Applies privacy-preserving techniques	Needs to balance verifiability, consistency and privacy.

distinct categories: Centralized Ledger Databases (CLDs) - exemplified by LedgerDB-based Centralized Ledger Technology (CLT), and Permissioned Ledger Databases (PLDs) - represented by Hyperledger fabric, FalconDB, BlockchainDB, Chainify, and BigchainDB. The authors emphasise that databases rooted in ledger technology offer security against malicious acts and administer privacy management, making them particularly beneficial for healthcare, finance, and IoT networks. Further, from an enterprise standpoint, ledger technology fosters trustless collaboration among businesses. Hence, the application of ledger databases has the potential to influence many sectors by enhancing security and ensuring privacy.

Similarly, Lupaiescu et al. [185] analyse BigchainDB and Amazon QLDB's performance across centralised and decentralised databases. Their findings illuminate the merits and shortcomings of both approaches, offering crucial insights for professionals contemplating the commercial implementation of these technologies. The authors' thorough comparison reveals that both databases boast high transaction rates and minimal latency. However, while BigchainDB, as a decentralised system, allows for autonomous ledger copies, Amazon QLDB, being centralised, does not permit this. Moreover, BigchainDB accommodates owner-controlled assets, a feature absent in Amazon QLDB. When assessing ease of development, BigchainDB presents a challenge due to its complex node configuration process, whereas Amazon QLDB, operating on a serverless architecture that ensures automated storage and resource scaling, is perceived to offer a medium level of difficulty.

1) ADVANCES IN CENTRALISED LEDGER DATABASES

Table 8 provides a comprehensive overview of recent advancements in centralised ledger database solutions that have potential applicability in SRPS scenarios. Noteworthy among these solutions are LedgerDB, GlassDB, SQL Ledger, TAB1, and PReVer.

a: LedgerDB

In their work, Yang et al. [179] present LedgerDB, a centralised ledger database characterised by strong auditability and high throughput. This makes it an appealing alternative to permissioned blockchains. LedgerDB employs a centralised architecture and a stateless journal storage model to guarantee tamper-evidence and non-repudiation features, akin to blockchain systems. The system's multi-granularity verification and non-repudiation protocols mitigate the risk of malicious behaviour from users and Ledger Service Providers (LSP), eradicating the need to trust the LSP.

LedgerDB is integrated with a digital certification and Timestamp Authority (TSA) service, enabling judicial-level auditability. The system supports verifiable data removals without undermining verifiability. Its data removal operators, ''purge'' and ''occult'', can remove outdated records or hide record content while maintaining verifiability.

In terms of performance, LedgerDB surpasses other systems like Hyperledger Fabric, achieving around 83x and 17x higher write and read throughput, respectively, and significantly lower latency. This performance, along with strong auditability and user-friendliness, has led many Alibaba Cloud customers to switch to LedgerDB.

The authors also introduced Dasein Verification to formalise ledger auditing and a Fractal Accumulating Model (FAM) to accelerate existence verification [186]. The FAM offers high verification performance with low storage overhead.

Lastly, LedgerDB can support verifiable data mutations via an ''occult'' operation, which allows the deletion of regulation-violated data without compromising the ledger's integrity, a feature critical for ledger systems needing to comply with regulations and privacy laws.

b: GlassDB

Yue et al. [180] highlight three limitations of LedgerDB that result in high verification costs. These include a large binary Accumulating Merkle Tree (bAMT) size due to storing one transaction per leaf, the costly verification of a key's value due to the unprotected clue index, and the linearly increasing proof size for multiple keys. To overcome these limitations, they introduced GlassDB.

GlassDB, as per the authors, combines high performance with verifiability, thanks to three innovative design aspects. First, it employs hash-protected index structures, offering comprehensive and efficient protection of the indexes, thus ensuring the database's integrity without significant overheads. Second, it batches independent operations from concurrent transactions, reducing disk-based operations and enhancing the system's throughput. Lastly, it adopts a concurrency control mechanism for transactions that maintain the database's ACID properties, allowing concurrent transactions to execute while upholding consistency and isolation.

Despite being designed for a distributed environment, GlassDB can be deployed in a centralised setting, with all nodes located within a single data centre or machine. While features like partitioning and two-phase commit might be unnecessary in this case, GlassDB's verifiability and efficiency advantages remain beneficial. Thus, GlassDB's design results in high throughput and reduced verification costs, qualifying it as an efficient and verifiable ledger database system.

c: SQL LEDGER

Antonopoulos et al. [181] presented SQL Ledger, an innovative technology that offers cryptographic verification of the integrity of relational data stored in Azure SQL Database and SQL Server. SQL Ledger ensures cryptographic data integrity by storing all historical data in the database and persisting its SHA-256 cryptographic digests in an unalterable, tamper-evident ledger. The technology offers a level of integrity protection known as Forward Integrity. This assumes that the RDBMS is trusted up until a transaction is processed, safeguarding against future attacks. This protection is suitable for many real-world applications where the data-hosting organisation must prove data authenticity and that it has not been tampered with.

SQL Ledger provides considerable benefits over traditional trust-establishing solutions that rely on audits or mediators. It is cheaper and more secure and retains the robustness, flexibility, and performance of a commercial RDBMS. These advantages make SQL Ledger an attractive choice for organisations requiring a balance of security and functionality in their database solutions. The technology uses core data structures from blockchain technology to capture the state of the database in compact cryptographic digests. These digests, which can be stored externally or shared with parties needing to validate data integrity, can be used later to confirm that data hasn't been tampered with. SQL Ledger also ensures Forward Integrity by utilising tamper-evident data structures and an asynchronous verification process, guaranteeing protection from tampering for historical data and cryptographic digests.

d: TAB1

Pathak et al. [182] introduced a Trust-Based ABAC in Edge-IoT networks (TAB1) mechanism using Blockchain technology to implement comprehensive security in resource-constrained IoT networks. TAB1 utilises access control and trust evaluation mechanisms to counter the impact of malicious IoT users and devices and integrates permissioned Hyperledger blockchain technology for enhanced security through authentication. The authors acknowledged the high overheads and energy-expensive operations associated with implementing blockchain technology directly on IoT networks, which often have limited computational power. TAB1 addresses this challenge using edge computing technology, implementing the trust evaluation mechanism as a Trust Calculation Contract (TCC) on edge devices with Hyperledger Composer. Additionally, an Attribute-based Access Control (ABAC) mechanism is implemented on the Hyperledger blockchain through two smart contracts.

The trust evaluation mechanism calculates the trust value of each IoT device based on behaviour and interactions, factoring in the device's transaction history, reputation, and feedback from other network devices. This system can detect and isolate malicious IoT users and devices, reducing their trust value and making it more difficult for them to participate in the network and launch further attacks. Although TAB1 isn't a centralised database as it employs Hyperledger blockchain technology, its access control and trust evaluation mechanisms could be adapted for other types of secure data storage and access control systems.

e: PReVer

Amiri et al. [183] introduced PReVer, a comprehensive framework that manages regulated dynamic data in a privacy-centric way. Overcoming many challenges, including verifying and applying updates, maintaining data consistency, and preserving privacy, PReVer provides consistent and verifiable execution of updates. As updates arrive, PReVer uses mechanisms to ensure they comply with regulations set forth by external bodies or constraints by internal authorities. After successful verification, these updates are implemented within the databases. Subsequently, PReVer offers techniques that ensure the databases remain free from corruption. To realise this, PReVer harnesses various privacy-preserving methods, such as fully homomorphic encryption for single database contexts, secure multi-party computation or token-based mechanisms for federated database environments, and private information retrieval for public data.

PReVer employs append-only ledgers as an unalterable, verifiable data structure, utilising centralised ledger databases and permissioned blockchains as its foundational infrastructure for single and verified database settings, respectively. Depending on the unique use case and requirements, PReVer can be applied in both centralised ledger databases and permissioned blockchain systems.

2) ENHANCING SRPS DATA INTEGRITY IN 5G NETWORKS THROUGH CENTRALISED LEDGER DATABASES

Centralised ledger databases can contribute to SRPS data integrity in 5G networks in the following ways:

a: DATA CONSISTENCY

Centralised ledgers maintain a single, consistent copy of all data entries. This makes it easier to ensure data integrity as all changes are instantly reflected across the whole system.

In 5G networks, this can ensure that all nodes and users have access to the most recent and accurate data.

b: TRANSACTION VALIDATION

Centralised ledgers can validate each transaction before it's recorded. This can prevent incorrect or fraudulent data from being added to the network. Given the diverse and numerous devices that may be connected in a 5G network, this ability to validate transactions can significantly enhance data integrity.

c: DATA RECOVERY

Centralised ledgers often maintain backup and recovery processes, which can help to restore data in case of system failures or data loss, maintaining the overall data integrity.

d: AUDIT TRAIL

Centralised ledgers maintain a complete history of all transactions, providing a comprehensive audit trail. This can be crucial for identifying and resolving data discrepancies, errors, or fraudulent activities, thus maintaining data integrity.

e: SECURITY

Centralised databases are controlled by a single authority, making implementing and monitoring security measures, including access control, encryption, and intrusion detection systems easier. These can protect the integrity of data by preventing unauthorised access or tampering.

VII. INSIGHTS GAINED, OPEN ISSUES AND RECOMMENDATIONS

This section presents the lessons learned, future research directions and the conclusion of this paper.

A. INSIGHTS GAINED FROM THIS SURVEY

This survey has provided several valuable insights into the security threats and challenges facing 5G networks for SRPS. Some of the key insights include:

1) The security threats to 5G networks for SRPS are diverse and encompass cybersecurity, physical, social, supply chain, and public space threats. However, past studies have focused mainly on cybersecurity threats, with limited attention paid to the other threat types. Additionally, few studies have addressed the specific use case of SRPS.
2) SRPS use cases have unique quality of service (QoS) requirements that are not adequately addressed in current 3GPP research studies. Unlike enhanced mobile broadband (eMBB) use cases, which require high data rates in the downlink, SRPS use cases require high data rates in the uplink.
3) The 3GPP security architecture and procedures for 5G systems were not designed with the particular use case of SRPS in mind. However, 3GPP has identified this need and is planning future studies to address it (Study of network for service robots with ambient intelligence FS_SOBOT [4]).
4) The threat landscape for SRPS will continue to evolve, highlighting the need for a continuous threat landscape-based software development and product design process for this unique use case.
5) The 5G-enabled WAN of SRPS is heterogeneous, employing various enabling technologies, which presents significant interoperability, migration, storage, and security challenges.
6) The 5G access network is more vulnerable to intrusion and threats, which could lead to objective security violations.
7) Although various security solutions exist for 5G-enabled wireless networks, focusing mainly on mMTC and IoT systems, there are still very few research results on SRPS use cases.
8) To address these challenges, adequate security measures should be introduced at the SRPS hardware, firmware, software, and infrastructure design stage.

B. OPEN ISSUES

Several open research problems require future research efforts for 5G networks for SRPS. Some of these include:

1) **Threat modelling and risk analysis:** There is a need for a comprehensive and systematic threat modelling and risk analysis framework for SRPS. This will enable researchers to identify and evaluate the risks associated with different attack scenarios and develop effective mitigation strategies.
2) **Real-time threat detection and response:** The real-time detection and response to security threats are crucial for protecting SRPS. Researchers need to develop real-time detection algorithms and response mechanisms to enable quick responses to attacks.
3) **Privacy protection:** Privacy protection is a significant concern for SRPS, as they interact with people and collect sensitive data. Researchers need to develop effective privacy protection mechanisms that can ensure the privacy of users' data.
4) **Secure communication protocols:** Communication between SR and other devices in public spaces is vulnerable to various attacks. There is a need for secure communication protocols that can protect against eavesdropping, interception, and other attacks.
5) **Resource-constrained devices:** SR and other devices in public spaces are often resource-constrained, making it challenging to implement resource-intensive security mechanisms. Researchers must develop lightweight security mechanisms that can operate efficiently on resource-constrained devices.
6) **Scalability:** As the number of SRPS increases, there is a need for scalable security solutions that can handle the increasing number of devices and users.
7) **Human factors:** SRPS interact with people, making it necessary to consider human factors in security design. Researchers must consider human behaviour,

perception, and cognition in developing security solutions for SRPS.

8) **Optimal management of the heterogeneous nature of 5G-enabled RAN for SRPS and their interoperability:** Given the wide range of technologies employed in the 5G network, including WiMAX, OFDMA networks, and WLAN, optimal management and integration of these technologies is a challenge that requires further research efforts.
9) **Secure embedded physical layer security in SR hardware, firmware, software and infrastructure:** Secure communication between SR and users' devices requires secure embedded physical layer security mechanisms. These mechanisms must be integrated into SR hardware, firmware, software, and infrastructure to provide robust protection against attacks.
10) **Optimal tradeoff between using post-quantum cryptographic security solutions and battery consumption for SRPS:** Post-quantum cryptographic security solutions are becoming increasingly popular due to their resistance to quantum computing attacks. However, such solutions can significantly impact battery consumption, which is a critical consideration for SRPS. Therefore, there is a need to explore optimal tradeoffs between using post-quantum cryptographic security solutions and battery consumption in SR.
11) **SRPS security framework:** There is a need for a specific security framework for SRPS use cases.

Addressing these research problems will help ensure SR security and privacy in public spaces and enable safe and effective deployment of these devices.

C. RECOMMENDATIONS

The following are some recommendations for 5G networks designed for SRPS use cases

1) The implementation of 3GPP SA 3 standards should be strictly followed, including adopting optional requirements to ensure maximum security.
2) Proper physical security of access network infrastructures should be ensured to achieve a robust 5G network system.
3) To ensure the proper functioning and guarantee social and public space performance, 5G networks for SRPS should always guarantee the required QoS (Quality of Service). This can be achieved through use case QoS design.
4) To ensure reliability, guaranteed QoS, and availability, redundancy in the form of alternative network communication sources, such as satellite communication, should be provided for SRPS.
5) Network design, configuration, and deployments should comply with best practices such as PKI (Public Key Infrastructure), virtualisation hardening, network segmentation, and protection for internal and external accesses.
6) Strong encryption and integrity protection algorithms should be used for signalling and user data transmission to ensure data confidentiality and integrity.
7) Correct implementation of 5G AKA (Authentication and Key Agreement) and EAP (Extensible Authentication Protocol) is critical for SRPS use cases.
8) A secure network and transport layer protocol should be implemented to ensure confidentiality, integrity, and replay protection in SRPS use cases.
9) From the start, security features should be incorporated into SRPS product and software development processes.
10) Rigorous testing, regular vulnerability assessments, and penetration testing should be conducted on all SRPS 5G network components and equipment.

By addressing these research problems, it will be possible to develop a comprehensive security framework for 5G networks for SRPS, enhancing the protection of both the network infrastructure and the users.

VIII. CONCLUSION

In conclusion, this survey has revealed various security threats that SRPS face in 5G networks. These threats include cybersecurity, physical, social, supply chain, and public space threats. Cybersecurity threats have received more attention in past studies, while physical, social, supply chain, and public space threats have been relatively underexplored. Moreover, the 5G-enabled wide area network of SRPS is heterogeneous, making interoperability, migration, storage, and security very challenging.

It is essential to acknowledge that as SRPS evolve, so will their threat landscape. Therefore, there is a need for a continuous threat landscape-based software development and product design process for this unique use case. The 5G-enabled RAN is also more vulnerable to intrusion and threats, leading to security objectives violations.

Several open research problems require future research efforts for 5G networks for SRPS. These include comprehensive threat modelling and risk analysis, real-time threat detection and response, privacy protection, and secure communication protocols. Addressing these challenges will require an interdisciplinary approach and collaboration among researchers from different fields.

It is vital to ensure the security benefits of the 3GPP SA 3 standards and their correct implementation, including adopting optional requirements. Strong encryption and integrity protection algorithms should always be adopted for signalling and user data transmission to ensure data confidentiality and integrity. Furthermore, a secure network and transport layer protocol should be implemented to ensure confidentiality, integrity, and replay protection in SRPS use cases. Finally, SRPS hardware, firmware, software, and infrastructure should introduce adequate security measures at the design stage to address these challenges.

Overall, this survey provides a framework for identifying and evaluating the security threats facing SRPS in

5G networks. It is hoped that this survey will inspire further research and the development of effective mitigation strategies to ensure the security and privacy of SRPS.

Future work should focus on developing a threat model and security framework for a social robot operating as a tour guide in a city ferry. This approach will enable specific enabling technology and a more targeted approach to security instead of a generalized framework for all use cases of SRPS. The findings from such future research will contribute significantly to the development of secure and trustworthy SRPS, ensuring their full potential as an essential technology for enhancing the human experience and societal development.

REFERENCES

[1] T. B. Sheridan, "A review of recent research in social robotics," *Current Opinion Psychol.*, vol. 36, pp. 7–12, Dec. 2020. Accessed: Mar. 30, 2022, doi: 10.1016/j.copsyc.2020.01.003.

[2] S. O. Oruma, M. Sánchez-Gordón, R. Colomo-Palacios, V. Gkioulos, and J. K. Hansen, "A systematic review on social robots in public spaces: Threat landscape and attack surface," *Computers*, vol. 11, no. 12, p. 181, Dec. 2022. Accessed: Jan. 2, 2023, doi: 10.3390/computers11120181.

[3] *Feasibility Study on New Services and Markets Technology Enablers for Critical Communications, Stage; 1 (Release 14)*, document TR 22.862, Version 14.1.0, 3GPP, 2016. Accessed: Nov. 10, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3014

[4] *Study on Network of Service Robots With Ambient Intelligence (Release 19)*, document TR 22.916, Version 0.3.0, 3GPP, 2023. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4097

[5] E. Fosch-Villaronga, C. Lutz, and A. Tamò-Larrieux, "Gathering expert opinions for social robots' ethical, legal, and societal concerns: Findings from four international workshops," *Int. J. Social Robot.*, vol. 12, no. 2, pp. 441–458, 2020. Accessed: Aug. 1, 2022, doi: 10.1007/s12369-019-00605-z.

[6] E. Fosch-Villaronga and T. Mahler, "Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots," *Comput. Law Secur. Rev.*, vol. 41, Jul. 2021, Art. no. 105528. Accessed: Mar. 30, 2022, doi: 10.1016/j.clsr.2021.105528.

[7] G. Mazzeo and M. Staffa, "TROS: Protecting humanoids ROS from privileged attackers," *Int. J. Social Robot.*, vol. 12, no. 3, pp. 827–841, Jul. 2020. Accessed: Mar. 30, 2022, doi: 10.1007/s12369-019-00581-4.

[8] *ENISA Threat Landscape for 5G Networks, Updated Threat Assessment for the 5th Generation of Mobile Telecommunications Networks (5G)*, Eur. Union Agency Cybersec., Athens, Greece, 2020. Accessed: Apr. 7, 2023, doi: 10.2824/802229.

[9] S. P. Rao, H.-Y. Chen, and T. Aura, "Threat modeling framework for mobile communication systems," *Comput. Secur.*, vol. 125, Feb. 2023, Art. no. 103047. Accessed: Apr. 7, 2023, doi: 10.1016/j.cose.2022.103047.

[10] B. Santos, L. Barriga, B. Dzogovic, I. Hassan, B. Feng, N. Jacot, V. T. Do, and T. Van Do, "Threat modelling for 5G networks," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, May 2022, pp. 611–616, doi: 10.1109/IWCMC55113.2022.9825149.

[11] A. Dutta and E. Hammad, "5G security challenges and opportunities: A system approach," in *Proc. IEEE 3rd 5G World Forum (5GWF)*, Sep. 2020, pp. 109–114, doi: 10.1109/5GWF49715.2020.9221122.

[12] F. Tian, P. Zhang, and Z. Yan, "A survey on C-RAN security," *IEEE Access*, vol. 5, pp. 13372–13386, 2017, doi: 10.1109/ACCESS.2017.2717852.

[13] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018, doi: 10.1109/MCOMSTD.2018.1700063.

[14] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Survey on multi-access edge computing security and privacy," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1078–1124, 2nd Quart., 2021, doi: 10.1109/COMST.2021.3062546.

[15] P. Ranaweera, A. Jurcut, and M. Liyanage, "MEC-enabled 5G use cases: A survey on security vulnerabilities and countermeasures," *ACM Comput. Surv.*, vol. 54, no. 9, pp. 1–37, Oct. 2021. Accessed: Nov. 3, 2022, doi: 10.1145/3474552.

[16] C. Paquin, D. Stebila, and G. Tamvada, "Benchmarking post-quantum cryptography in TLS," in *Post-Quantum Cryptography* (Lecture Notes in Computer Science), J. Ding and J.-P. Tillich, Eds. Cham, Switzerland: Springer, 2020, pp. 72–91, doi: 10.1007/978-3-030-44223-1_5.

[17] Z. Lv, L. Qiao, and Q. Wang, "Cognitive robotics on 5G networks," *ACM Trans. Internet Technol.*, vol. 21, no. 4, pp. 1–18, Jul. 2021. Accessed: Nov. 3, 2022, doi: 10.1145/3414842.

[18] M. Sarrica, S. Brondi, and L. Fortunati, "How many facets does a 'social robot' have? A review of scientific and popular definitions online," *Inf. Technol. People*, vol. 33, no. 1, pp. 1–21, Apr. 2019. Accessed: Jul. 8, 2022, doi: 10.1108/ITP-04-2018-0203.

[19] U. S. P. S. Aditya, R. Singh, P. K. Singh, and A. Kalla, "A survey on blockchain in robotics: Issues, opportunities, challenges and future directions," *J. Netw. Comput. Appl.*, vol. 196, Dec. 2021, Art. no. 103245. Accessed: Mar. 30, 2022, doi: 10.1016/j.jnca.2021.103245.

[20] M. Joosse, M. Lohse, N. V. Berkel, A. Sardar, and V. Evers, "Making appearances: How robots should approach people," *ACM Trans. Hum.-Robot Interact.*, vol. 10, no. 1, pp. 1–24, Mar. 2021. Accessed: Aug. 13, 2022, doi: 10.1145/3385121.

[21] K. Dautenhahn, "Methodology & themes of human–robot interaction: A growing research field," *Int. J. Adv. Robot. Syst.*, vol. 4, no. 1, p. 15, Mar. 2007. Accessed: Oct. 8, 2022, doi: 10.5772/5702.

[22] O. Mubin, M. I. Ahmad, S. Kaur, W. Shi, and A. Khan, "Social robots in public spaces: A meta-review," in *Social Robotics* (Lecture Notes in Computer Science), S. S. Ge, J.-J. Cabibihan, M. A. Salichs, E. Broadbent, H. He, A. R. Wagner, and A. Castro-González, Eds. Cham, Switzerland: Springer, 2018, pp. 213–220, doi: 10.1007/978-3-030-05204-1_21.

[23] M. V. Tonkin, "Socially responsible design for social robots in public spaces," Ph.D. thesis, 2021.

[24] L. Fortunati, F. Cavallo, and M. Sarrica, "The role of social robots in public space," in *Ambient Assisted Living* (Lecture Notes in Electrical Engineering), N. Casiddu, C. Porfirione, A. Monteriù, and F. Cavallo, Eds. Cham, Switzerland: Springer, 2019, pp. 171–186, doi: 10.1007/978-3-030-04672-9_11.

[25] I. Altman and E. H. Zube, *Public Places and Spaces*. New York, NY, USA: Springer, Dec. 2012, p. 329.

[26] T. Belpaeme, J. Kennedy, A. Ramachandran, B. Scassellati, and F. Tanaka, "Social robots for education: A review," *Sci. Robot.*, vol. 3, no. 21, Aug. 2018, Art. no. eaat5954. Accessed: Jul. 8, 2022, doi: 10.1126/scirobotics.aat5954.

[27] R. B. Rosenberg-Kima, Y. Koren, and G. Gordon, "Robot-supported collaborative learning (RSCL): Social robots as teaching assistants for higher education small group facilitation," *Front. Robot. AI*, vol. 6, pp. 1–12, Jan. 2020. Accessed: Jul. 8, 2022, doi: 10.3389/frobt.2019.00148.

[28] C. Lytridis, C. Bazinas, G. Sidiropoulos, G. A. Papakostas, V. G. Kaburlasos, V.-A. Nikopoulou, V. Holeva, and A. Evangeliou, "Distance special education delivery by social robots," *Electronics*, vol. 9, no. 6, p. 1034, Jun. 2020. Accessed: Jul. 8, 2022, doi: 10.3390/electronics9061034.

[29] J. Kanero, V. Geçkin, C. Oranç, E. Mamus, A. C. Küntay, and T. Göksun, "Social robots for early language learning: Current evidence and future directions," *Child Develop. Perspect.*, vol. 12, no. 3, pp. 146–151, Sep. 2018. Accessed: Jul. 8, 2022, doi: 10.1111/cdep.12277.

[30] R. van den Berghe, J. Verhagen, O. Oudgenoeg-Paz, S. van der Ven, and P. Leseman, "Social robots for language learning: A review," *Rev. Educ. Res.*, vol. 89, no. 2, pp. 259–295, Apr. 2019. Accessed: Jul. 8, 2022, doi: 10.3102/0034654318821286.

[31] T. Belpaeme et al., "Guidelines for designing social robots as second language tutors," *Int. J. Social Robot.*, vol. 10, no. 3, pp. 325–341, Jun. 2018. Accessed: Jul. 8, 2022, doi: 10.1007/s12369-018-0467-6.

[32] D. E. Logan, C. Breazeal, M. S. Goodwin, S. Jeong, B. O'Connell, D. Smith-Freedman, J. Heathers, and P. Weinstock, ''Social robots for hospitalized children,'' *Pediatrics*, vol. 144, no. 1, Jul. 2019, Art. no. e20181511. Accessed: Jul. 8, 2022, doi: 10.1542/peds.2018-1511.

[33] N. L. Robinson, T. V. Cottier, and D. J. Kavanagh, ''Psychosocial health interventions by social robots: Systematic review of randomized controlled trials,'' *J. Med. Internet Res.*, vol. 21, no. 5, May 2019, Art. no. e13203. Accessed: Mar. 27, 2023, doi: 10.2196/13203.

[34] S. Chen, C. Jones, and W. Moyle, ''Social robots for depression in older adults: A systematic review,'' *J. Nursing Scholarship*, vol. 50, no. 6, pp. 612–622, Nov. 2018. Accessed: Mar. 27, 2023, doi: 10.1111/jnu.12423.

[35] A. A. Scoglio, E. D. Reilly, J. A. Gorman, and C. E. Drebing, ''Use of social robots in mental health and well-being research: Systematic review,'' *J. Med. Internet Res.*, vol. 21, no. 7, Jul. 2019, Art. no. e13322. Accessed: Jul. 8, 2022, doi: 10.2196/13322.

[36] S. G. Alonso, S. Hamrioui, I. D. L. T. Díez, E. M. Cruz, M. López-Coronado, and M. Franco, ''Social robots for people with aging and dementia: A systematic review of literature,'' *Telemed. E-Health*, vol. 25, no. 7, pp. 533–540, Jul. 2019. Accessed: Mar. 27, 2023, doi: 10.1089/tmj.2018.0051.

[37] A. Niculescu, B. van Dijk, A. Nijholt, and S. L. See, ''The influence of voice pitch on the evaluation of a social robot receptionist,'' in *Proc. Int. Conf. User Sci. Eng. (i-USEr)*, Nov. 2011, pp. 18–23, doi: 10.1109/iUSEr.2011.6150529.

[38] M. Hellou, J. Lim, N. Gasteiger, M. Jang, and H. S. Ahn, ''Technical methods for social robots in museum settings: An overview of the literature,'' *Int. J. Social Robot.*, vol. 14, no. 8, pp. 1767–1786, Oct. 2022. Accessed: Mar. 27, 2023, doi: 10.1007/s12369-022-00904-y.

[39] J. Nakanishi, I. Kuramoto, J. Baba, K. Ogawa, Y. Yoshikawa, and H. Ishiguro, ''Continuous hospitality with social robots at a hotel,'' *Social Netw. Appl. Sci.*, vol. 2, no. 3, p. 452, Mar. 2020. Accessed: Mar. 27, 2023, doi: 10.1007/s42452-020-2192-7.

[40] O. H. Chi, S. Jia, Y. Li, and D. Gursoy, ''Developing a formative scale to measure consumers' trust toward interaction with artificially intelligent (AI) social robots in service delivery,'' *Comput. Hum. Behav.*, vol. 118, May 2021, Art. no. 106700. Accessed: Jul. 10, 2022, doi: 10.1016/j.chb.2021.106700.

[41] J. M. Garcia-Haro, E. D. Oña, J. Hernandez-Vicen, S. Martinez, and C. Balaguer, ''Service robots in catering applications: A review and future challenges,'' *Electronics*, vol. 10, no. 1, p. 47, Dec. 2020. Accessed: Jul. 10, 2022, doi: 10.3390/electronics10010047.

[42] L. Aymerich-Franch and I. Ferrer, ''Social robots as a brand strategy,'' in *Innovation in Advertising and Branding Communication*. Oxfordshire, U.K.: Routledge, 2020.

[43] C. Lytridis, C. Bazinas, V. G. Kaburlasos, V. Vassileva-Aleksandrova, M. Youssfi, M. Mestari, V. Ferelis, and A. Jaki, ''Social robots as cyber-physical actors in entertainment and education,'' in *Proc. Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, Sep. 2019, pp. 1–6, doi: 10.23919/SOFTCOM.2019.8903630.

[44] T. Chikaraishi, Y. Yoshikawa, K. Ogawa, O. Hirata, and H. Ishiguro, ''Creation and staging of android theatre 'Sayonar' towards developing highly human-like robots,'' *Future Internet*, vol. 9, no. 4, p. 75, Nov. 2017, doi: 10.3390/fi9040075.

[45] N. S. Jecker, ''Nothing to be ashamed of: Sex robots for older adults with disabilities,'' *J. Med. Ethics*, vol. 47, no. 1, pp. 26–32, Jan. 20213 Accessed: Mar. 27, 2023, doi: 10.1136/medethics-2020-106645.

[46] *Security Architecture and Procedures for 5G System (Release 18)*, document TS 33.501, Version 18.0.0, 3GPP, 2023. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

[47] Y. Ji, J. Zhang, Y. Xiao, and Z. Liu, ''5G flexible optical transport networks with large-capacity, low-latency and high-efficiency,'' *China Commun.*, vol. 16, no. 5, pp. 19–32, May 2019, doi: 10.23919/j.cc.2019.05.002.

[48] S. Bhattacharjee, R. Schmidt, K. Katsalis, C.-Y. Chang, T. Bauschert, and N. Nikaein, ''Time-sensitive networking for 5G fronthaul networks,'' in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–7, doi: 10.1109/ICC40277.2020.9149161.

[49] M. Cai, Q. Liu, and H. Jiang, ''A novel efficient wireless fronthaul (EWF) method for the common public radio interface (CPRI) signal transmission,'' in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Aug. 2018, pp. 1–5, doi: 10.1109/VTCFall.2018.8690747.

[50] L. Li, M. Bi, H. Xin, Y. Zhang, Y. Fu, X. Miao, A. M. Mikaeil, and W. Hu, ''Enabling flexible link capacity for eCPRI-based fronthaul with load-adaptive quantization resolution,'' *IEEE Access*, vol. 7, pp. 102174–102185, 2019, doi: 10.1109/ACCESS.2019.2930214.

[51] A. S. Abdalla, P. S. Upadhyaya, V. K. Shah, and V. Marojevic, ''Toward next generation open radio access networks: What O-RAN can and cannot do!'' *IEEE Netw.*, vol. 36, no. 6, pp. 206–213, Nov. 2022, doi: 10.1109/MNET.108.2100659.

[52] J. Yu, Y. Li, M. Bhopalwala, S. Das, M. Ruffini, and D. C. Kilper, ''Midhaul transmission using edge data centers with split PHY processing and wavelength reassignment for 5G wireless networks,'' in *Proc. Int. Conf. Opt. Netw. Design Modeling (ONDM)*, May 2018, pp. 178–183, doi: 10.23919/ONDM.2018.8396127.

[53] M. Jaber, M. A. Imran, R. Tafazolli, and A. Tukmanov, ''5G backhaul challenges and emerging research directions: A survey,'' *IEEE Access*, vol. 4, pp. 1743–1766, 2016, doi: 10.1109/ACCESS.2016.2556011.

[54] A. Omri, M. Shaqfeh, A. Ali, and H. Alnuweiri, ''Synchronization procedure in 5G NR systems,'' *IEEE Access*, vol. 7, pp. 41286–41295, 2019, doi: 10.1109/ACCESS.2019.2907970.

[55] *Catalogue of General Security Assurance Requirements (Release 17)*, document TS 33.117, Version 17.2.0, 3GPP, 2023. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2928

[56] *Security Assurance Specification (SCAS) for the Next Generation Node B (gNodeB) Network Product Class (Release 17)*, document TS 33.511, Version 17.3.1, 3GPP, 2022, [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3444

[57] *5G Security Assurance Specification (SCAS); Access and Mobility Management Function (AMF) (Release 17)*, document TS 33.512, Version 17.3.0, 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3445

[58] *5G Security Assurance Specification (SCAS); User Plane Function (UPF) (Release 17)*, document TS 33.513, Version 17.1.0, 3GPP, 2023. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3446

[59] *5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) Network Product Class (Release 17)*, document TS 33.514, Version 17.0.0, 3GPP, 2021. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3447

[60] *5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) Network Product Class (Release 17)*, document TS 33.515, Version 17.0.0, 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3448

[61] *5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) Network Product Class (Release 17)*, document TS 33.516, Version 17.0.0, 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3535

[62] *5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) Network Product Class (Release 17)*, document TS 33.517, Version 17.0.0, 3GPP, 2021. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3536

[63] *5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) Network Product Class (Release 17)*, document TS 33.518, Version 17.0.0, 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3537

[64] *5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) Network Product Class (Release 17)*, document TS 33.519, Version 17.0.0, 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3538

[65] *5G Security Assurance Specification (SCAS); Non-3GPP InterWorking Function (N3IWF) (Release 17)*, document TS 33.520, Version 0.3.0, 3GPP, 2021. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3748

[66] *5G Security Assurance Specification (SCAS);Network Data Analytics Function (NWDAF) (Release 17)*, document TS 33.521, Version 17.2.0, 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/Specification Details.aspx?specificationId=3749

[67] *5G SCAS; Service Communication Proxy (SECOP)*, document TS 33.522, Version 17.1.0, 3GPP, 2021. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/Specification Details.aspx?specificationId=3750

[68] *Study on Lawful Interception (LI) Service in 5G (Release 15)*, document TR 33.842, 3GPP, 2017. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/Specification Details.aspx?specificationId=3184

[69] *Lawful Interception Requirements (Release 18)*, document TS 33.126, Version 18.0.0, 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/Specification Details.spx?specificationId=3181

[70] *Lawful Interception (LI) Architecture and Functions (Release 18)*, document TS 33.127, Version 18.2.0, 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/Specification Details.aspx?specificationId=3182

[71] *Security; Protocol and Procedures for Lawful Interception (LI); Stage 3 (Release 18)*, document TS 33.128, Version 18.2.0, 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3183

[72] *Study on Security Aspects of 5G Network Slicing Management (Release 15)*, document TR 33.811, Version 15.0.0, 3GPP, 2018. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3358

[73] *Study on Security Aspects of Enhancement of Support for Edge Computing in the 5G Core (5GC) (Release 17)*, document TR 33.839, Version 17.1.0, 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/Specification Details.aspx?specificationId=3759

[74] *Study on Security Enhancements of 5G System (5GS) for Vertical and Local Area Network (LAN) Services (Release 16)*, document TR 33.819, Version 16.1.0, 3GPP, 2020. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/Specification Details.aspx?specificationId=3544

[75] *Study on 5G Security Enhancements Against False Base Stations (FBS) (Release 16)*, document TR 33.809, Version 0.20.0, 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539

[76] *Study on key Issues and Potential Solutions for Integrity Protection of the User Plane (UP) (Release 17)*, document TR 33.853, Version 17.0.0, 3GPP, 2021. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/Specification Details.aspx?specificationId=3571

[77] *Study on Authentication Enhancements in the 5G System (5GS) (Release 17)*, document TR 33.846, Version 17.0.0, 3GPP, 2021. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3573

[78] *Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP Virtualized Network Products (Release 17)*, document TR 33.818, Version 17.1.0, 3GPP, 2021. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/Specification Details.aspx?specificationId=3543

[79] *Security Aspects of Machine-Type Communications (MTC) and Other Mobile Data Applications Communications Enhancements (Release 17)*, document TS 33.187, Version 7.0.0, 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/Specification Details.aspx?specificationId=2274

[80] *Proximity-Based Services (ProSe); Security Aspects (Release 14)*, document TS 33.303, Version 14.1.0, 3GPP, 2017. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/Specification Details.aspx?specificationId=2292

[81] *Security Aspects of 3GPP Support for Advanced Vehicle-to-Everything (V2X) Services (Release 17)*, document TS 33.536, Version 17.1.0, 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3724

[82] *Authentication and Key Management for Applications (AKMA) Based on 3GPP Credentials in the 5G System (5GS) (Release 17)*, document TS 33.535, Version 17.7.0, 3GPP, 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/Specification Details.aspx?specificationId=3690

[83] *Security Aspects of Common API Framework (CAPIF) for 3GPP Northbound APIs (Release 16)*, document TS 33.112, Version 16.4.0, 3GPP, 2023. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3420

[84] 3GPP. (2022). *3GPP Partners*. Accessed: Apr. 5, 2023. [Online]. Available: https://www.3gpp.org/about-us/partners

[85] 3GPP Groups. (2023). *The Technical Specification Groups (TSGs)*. Accessed: Apr. 5, 2023. [Online]. Available: https://www.3gpp.org/3gpp-groups

[86] S. Sirotkin, *5G Radio Access Network Architecture: The Dark Side of 5G,*, 1st ed. Hoboken, NJ, USA: Wiley, 2021, p. 451. [Online]. Available: https://lccn.loc.gov/2020020729

[87] D. M. Abdullah and S. Y. Ameen, "Enhanced mobile broadband (EMBB): A review," *J. Inf. Technol. Informat.*, vol. 1, no. 1, pp. 13–19, 2021.

[88] S. R. Pokhrel, J. Ding, J. Park, O. Park, and J. Choi, "Towards enabling critical mMTC: A review of URLLC within mMTC," *IEEE Access*, vol. 8, pp. 131796–131813, 2020, doi: 10.1109/ACCESS.2020.3010271.

[89] M. A. Siddiqi, H. Yu, and J. Joung, "5G ultra-reliable low-latency communication implementation challenges and operational issues with IoT devices," *Electronics*, vol. 8, no. 9, p. 981, Sep. 2019, doi: 10.3390/electronics8090981.

[90] C. Shin, E. Farag, H. Ryu, M. Zhou, and Y. Kim, "Vehicle-to-everything (V2X) evolution from 4G to 5G in 3GPP: Focusing on resource allocation aspects," *IEEE Access*, vol. 11, pp. 18689–18703, 2023, doi: 10.1109/ACCESS.2023.3247127.

[91] L. Guevara and F. A. Cheein, "The role of 5G technologies: Challenges in smart cities and intelligent transportation systems," *Sustainability*, vol. 12, no. 16, p. 6469, Aug. 2020, doi: 10.3390/su12166469.

[92] A. Mahmood, L. Beltramelli, S. F. Abedin, S. Zeb, N. I. Mowla, S. A. Hassan, E. Sisinni, and M. Gidlund, "Industrial IoT in 5G-and-beyond networks: Vision, architecture, and design trends," *IEEE Trans. Ind. Informat.*, vol. 18, no. 6, pp. 4122–4137, Jun. 2022, doi: 10.1109/TII.2021.3115697.

[93] M. Berlet, T. Vogel, M. Gharba, J. Eichinger, E. Schulz, H. Friess, D. Wilhelm, D. Ostler, and M. Kranzfelder, "Emergency telemedicine mobile ultrasounds using a 5G-enabled application: Development and usability study," *JMIR Formative Res.*, vol. 6, no. 5, May 2022, Art. no. e36824, doi: 10.2196/36824.

[94] W. A. S. Katsigiannis and N. Ramzan, "5G: Disruption in media and entertainment," in *Enabling 5G Communication Systems to Support Vertical Industries*. Hoboken, NJ, USA: Wiley, 2019.

[95] M. Volk and J. Sterle, "5G experimentation for public safety: Technologies, facilities and use cases," *IEEE Access*, vol. 9, pp. 41184–41217, 2021, doi: 10.1109/ACCESS.2021.3064405.

[96] S. O. Oruma, S. Misra, and L. Fernandez-Sanz, "Agriculture 4.0: An implementation framework for food security attainment in Nigeria's post-COVID-19 era," *IEEE Access*, vol. 9, pp. 83592–83627, 2021, doi: 10.1109/ACCESS.2021.3086453.

[97] *IMT Vision Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond*, document ITU-R M.2083-0, ITU-R, 2015, p. 21. [Online]. Available: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf

[98] V.-G. Nguyen, A. Brunstrom, K.-J. Grinnemo, J. Taheri, M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Yliant-tilla, "5G mobile networks: Requirements enabling technologies and research activities," in *Comprehensive Guide to 5G Security*. Hoboken, NJ, USA: Wiley, 2018, pp. 31–57.

[99] E. Mohyeldin, "Minimum technical performance requirements for IMT-2020 radio interface(s)," NOKIA, Espoo, Finland, Tech. Rep. 2410-0, 2016, p. 12. [Online]. Available: https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Documents/S01-1_Requirements%20for%20IMT-2020_Rev.pdf

[100] *NR; User Equipment (UE) Radio Access Capabilities*, document TS 38.3063, Version 17.3.0, 3GPP, 2016. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/Specification Details.aspx?specificationId=3193

[101] Y. R. Li, B. Gao, X. Zhang, and K. Huang, "Beam management in millimeter-wave communications for 5G and beyond," *IEEE Access*, vol. 8, pp. 13282–13293, 2020, doi: 10.1109/ACCESS.2019.2963514.

[102] O. Elijah, S. K. A. Rahim, W. K. New, C. Y. Leow, K. Cumanan, and T. Kim Geok, "Intelligent massive MIMO systems for beyond 5G networks: An overview and future trends," *IEEE Access*, vol. 10, pp. 102532–102563, 2022, doi: 10.1109/ACCESS.2022.3208284.

[103] L. Rao, M. Pant, L. Malviya, A. Parmar, and S. V. Charhate, "5G beamforming techniques for the coverage of intended directions in modern wireless communication: In-depth review," *Int. J. Microw. Wireless Technol.*, vol. 13, no. 10, pp. 1039–1062, Dec. 2021, doi: 10.1017/S1759078720001622.

[104] M. De Ree, G. Mantas, A. Radwan, S. Mumtaz, J. Rodriguez, and I. E. Otung, "Key management for beyond 5G mobile small cells: A survey," *IEEE Access*, vol. 7, pp. 59200–59236, 2019, doi: 10.1109/ACCESS.2019.2914359.

[105] S. Zhang, "An overview of network slicing for 5G," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 111–117, Jun. 2019, doi: 10.1109/MWC.2019.1800234.

[106] N. Hassan, K. A. Yau, and C. Wu, "Edge computing in 5G: A review," *IEEE Access*, vol. 7, pp. 127276–127289, 2019, doi: 10.1109/ACCESS.2019.2938534.

[107] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," *Comput. Netw.*, vol. 167, Feb. 2020, Art. no. 106984, doi: 10.1016/j.comnet.2019.106984.

[108] Y. Yuan, Z. Yuan, and L. Tian, "5G non-orthogonal multiple access study in 3GPP," *IEEE Commun. Mag.*, vol. 58, no. 7, pp. 90–96, Jul. 2020, doi: 10.1109/MCOM.001.1900450.

[109] M. H. Adnan and Z. A. Zukarnain, "Device-to-device communication in 5G environment: Issues, solutions, and challenges," *Symmetry*, vol. 12, no. 11, p. 1762, Oct. 2020, doi: 10.3390/sym12111762.

[110] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong, and J. P. Jue, "All one needs to know about fog computing and related edge computing paradigms: A complete survey," *J. Syst. Archit.*, vol. 98, pp. 289–330, Sep. 2019, doi: 10.1016/j.sysarc.2019.02.009.

[111] M. Babar, M. S. Khan, F. Ali, M. Imran, and M. Shoaib, "Cloudlet computing: Recent advances, taxonomy, and challenges," *IEEE Access*, vol. 9, pp. 29609–29622, 2021, doi: 10.1109/ACCESS.2021.3059072.

[112] J. S. Preden, K. Tammemäe, A. Jantsch, M. Leier, A. Riid, and E. Calis, "The benefits of self-awareness and attention in fog and mist computing," *Computer*, vol. 48, no. 7, pp. 37–45, Jul. 2015, doi: 10.1109/MC.2015.207.

[113] European Partnership on Artificial Intelligence. (2021). *AI Data Robotics Partnership EU*. Accessed: Oct. 15, 2022. [Online]. Available: https://ai-data-robotics-partnership.eu/

[114] S. Sullivan, A. Brighente, S. A. P. Kumar, and M. Conti, "5G security challenges and solutions: A review by OSI layers," *IEEE Access*, vol. 9, pp. 116294–116314, 2021, doi: 10.1109/ACCESS.2021.3105396.

[115] R. P. Jover and V. Marojevic, "Security and protocol exploit analysis of the 5G specifications," *IEEE Access*, vol. 7, pp. 24956–24963, 2019, doi: 10.1109/ACCESS.2019.2899254.

[116] S. R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "LTEInspector: A systematic approach for adversarial testing of 4G LTE," in *Proc. Netw. Distrib. Syst. Secur. (NDSS) Symp.*, 2018, pp. 1–15, doi: 10.14722/ndss.2018.23313.

[117] M. Labib, V. Marojevic, J. H. Reed, and A. I. Zaghloul, "Extending LTE into the unlicensed spectrum: Technical analysis of the proposed variants," *IEEE Commun. Standards Mag.*, vol. 1, no. 4, pp. 31–39, Dec. 2017, doi: 10.1109/MCOMSTD.2017.1700040.

[118] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper, "Breaking LTE on layer two," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 1121–1136, doi: 10.1109/SP.2019.00006.

[119] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018, doi: 10.1016/j.future.2016.11.009.

[120] S. Wang, X. Zhang, Y. Zhang, L. Wang, J. Yang, and W. Wang, "A survey on mobile edge networks: Convergence of computing, caching and communications," *IEEE Access*, vol. 5, pp. 6757–6779, 2017, doi: 10.1109/ACCESS.2017.2685434.

[121] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017, doi: 10.1109/COMST.2017.2745201.

[122] X. Yang, Z. Chen, K. Li, Y. Sun, N. Liu, W. Xie, and Y. Zhao, "Communication-constrained mobile edge computing systems for wireless virtual reality: Scheduling and tradeoff," *IEEE Access*, vol. 6, pp. 16665–16677, 2018, doi: 10.1109/ACCESS.2018.2817288.

[123] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018, doi: 10.1109/ACCESS.2017.2778504.

[124] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for Internet of Things realization," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2961–2991, 4th Quart., 2018, doi: 10.1109/COMST.2018.2849509.

[125] D. Sabella, A. Vaillant, P. Kuure, U. Rauschenbach, and F. Giust, "Mobile-edge computing architecture: The role of MEC in the Internet of Things," *IEEE Consum. Electron. Mag.*, vol. 5, no. 4, pp. 84–91, Oct. 2016, doi: 10.1109/MCE.2016.2590118.

[126] S. Wang, J. Xu, N. Zhang, and Y. Liu, "A survey on service migration in mobile edge computing," *IEEE Access*, vol. 6, pp. 23511–23528, 2018, doi: 10.1109/ACCESS.2018.2828102.

[127] F. Zhang, G. Liu, X. Fu, and R. Yahyapour, "A survey on virtual machine migration: Challenges, techniques, and open issues," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1206–1243, 2nd Quart., 2018, doi: 10.1109/COMST.2018.2794881.

[128] J. Ren, D. Zhang, S. He, Y. Zhang, and T. Li, "A survey on end-edge-cloud orchestrated network computing paradigms: Transparent computing, mobile edge computing, fog computing, and cloudlet," *ACM Comput. Surv.*, vol. 52, no. 6, pp. 1–36, Oct. 2019. Accessed: Nov. 14, 2022, doi: 10.1145/3362031.

[129] I. Parvez, A. Rahmati, I. Guvenc, A. I. Sarwat, and H. Dai, "A survey on low latency towards 5G: RAN, core network and caching solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3098–3130, 4th Quart., 2018, doi: 10.1109/COMST.2018.2841349.

[130] X. Ji, K. Huang, L. Jin, H. Tang, C. Liu, Z. Zhong, W. You, X. Xu, H. Zhao, J. Wu, and M. Yi, "Overview of 5G security technology," *Sci. China Inf. Sci.*, vol. 61, no. 8, Aug. 2018, Art. no. 081301, doi: 10.1007/s11432-017-9426-4.

[131] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018, doi: 10.1109/ACCESS.2017.2779146.

[132] M. Nieles, K. Dempsey, and V. Y. Pillitteri, *An Introduction to Information Security*, Standard NIST SP 800-12, Revision 1, 2017. Accessed: Oct. 18, 2022. [Online]. Available: https://csrc.nist.gov/glossary/term/attack

[133] *Minimum Security Requirements for Federal Information and Information Systems*, Standard NIST FIPS PUB 200, NIST, 2006. Accessed: Oct. 17, 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

[134] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, *Guide to Industrial Control Systems (ICS) Security*, Standard NIST SP 800-82r2, National Institute of Standards and Technology, Jun. 2015. Accessed: Nov. 12, 2022, doi: 10.6028/NIST.SP.800-82r2.

[135] S. L. Garfinkel, *De-Identification of Personal Information*, Standard NIST IR 8053, National Institute of Standards and Technology, Oct. 2015. Accessed: Oct. 18, 2022, doi: 10.6028/NIST.IR.8053.

[136] T. Kumar, M. Liyanage, I. Ahmad, A. Braeken, and M. Ylianttila, "User privacy, identity and trust in 5G," in *A Comprehensive Guide to 5G Security*, M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, Eds. Hoboken, NJ, USA: Wiley, Jan. 2018, pp. 267–279. Accessed: Nov. 13, 2022, doi: 10.1002/9781119293071.ch12.

[137] S. S. Dhanda, B. Singh, and P. Jindal, "Demystifying elliptic curve cryptography: Curve selection, implementation and countermeasures to attacks," *J. Interdiscipl. Math.*, vol. 23, no. 2, pp. 463–470, Feb. 2020. Accessed: Nov. 12, 2022, doi: 10.1080/09720502.2020.1731959.

[138] S. Gupta, B. L. Parne, and N. S. Chaudhari, "Security vulnerabilities in handover authentication mechanism of 5G network," in *Proc. 1st Int. Conf. Secure Cyber Comput. Commun. (ICSCCC)*, Dec. 2018, pp. 369–374.

[139] H. Zhu and C. Huang, "Availability-aware mobile edge application placement in 5G networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6.

[140] O. Kodheli, J. Querol, A. Astro, S. Coloma, L. Rana, Z. Bokal, S. Kumar, C. M. Luna, J. Thoemel, J. C. M. Duncan, M. A. O. Mendez, S. Chatzinotas, and B. Ottersten, "5G space communications lab: Reaching new heights," in *Proc. 18th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2022, pp. 349–356, doi: 10.1109/DCOSS54816.2022.00063.

[141] P. Hao and X. Wang, "Integrating PHY security into NDN-IoT networks by exploiting MEC: Authentication efficiency, robustness, and accuracy enhancement," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 5, no. 4, pp. 792–806, Dec. 2019. Accessed: Nov. 12, 2022, doi: 10.1109/TSIPN.2019.2932678.

[142] G. Choudhary, J. Kim, and V. Sharma, "Security of 5G-mobile backhaul networks: A survey," *J. Wireless Mobility Netw., Ubiquitous Comput. Dependable Appl.*, vol. 9, no. 4, pp. 41–70, 2018. Accessed: Nov. 12, 2022, doi: 10.22667/JOWUA.2018.12.31.041.

[143] S. Cha, M. Chuang, K. Yeh, Z. Huang, and C. Su, "A user-friendly privacy framework for users to achieve consents with nearby BLE devices," *IEEE Access*, vol. 6, pp. 20779–20787, 2018, doi: 10.1109/ACCESS.2018.2820716.

[144] P. Gope, R. Amin, S. K. H. Islam, N. Kumar, and V. K. Bhalla, "Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment," *Future Gener. Comput. Syst.*, vol. 83, pp. 629–637, Jun. 2018. Accessed: Nov. 12, 2022, doi: 10.1016/j.future.2017.06.023.

[145] Y. Zhang, F. Ren, A. Wu, T. Zhang, J. Cao, and D. Zheng, "Certificateless multi-party authenticated encryption for NB-IoT terminals in 5G networks," *IEEE Access*, vol. 7, pp. 114721–114730, 2019, doi: 10.1109/ACCESS.2019.2936123.

[146] Z. Zhao, G. Min, Y. Pang, W. Gao, and J. Lv, "Towards fast and reliable WiFi authentication by utilizing visible light diversity," in *Proc. 16th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON)*, Jun. 2019, pp. 1–9, doi: 10.1109/SAHCN.2019.8824935.

[147] M. H. Mahalat, S. Saha, A. Mondal, and B. Sen, "A PUF based light weight protocol for secure WiFi authentication of IoT devices," in *Proc. 8th Int. Symp. Embedded Comput. Syst. Design (ISED)*, Dec. 2018, pp. 183–187, doi: 10.1109/ISED.2018.8703993.

[148] G. Li and P. Bours, "Studying WiFi and accelerometer data based authentication method on mobile phones," in *Proc. 2nd Int. Conf. Biometric Eng. Appl.*, May 2018, pp. 18–23, doi: 10.1145/3230820.3230824.

[149] I. Adam and J. Ping, "Framework for security event management in 5G," in *Proc. 13th Int. Conf. Availability, Rel. Secur.*, Aug. 2018, pp. 1–7. Accessed: Nov. 12, 2022, doi: 10.1145/3230833.3233254.

[150] V. Ruchkin, V. Fulin, V. Romanchuk, A. Koryachko, and E. Ruchkina, "Personal trusted platform module for the multi-core system of 5G security and privacy," in *Proc. ELEKTRO*, May 2020, pp. 1–4, doi: 10.1109/ELEKTRO49696.2020.9130294.

[151] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018, doi: 10.1109/ACCESS.2018.2801266.

[152] H. Jiang, J. Li, P. Zhao, F. Zeng, Z. Xiao, and A. Iyengar, "Location privacy-preserving mechanisms in location-based services: A comprehensive survey," *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–36, Jan. 2022. Accessed: Nov. 13, 2022, doi: 10.1145/3423165.

[153] H. Wang, C. Gao, Y. Li, G. Wang, D. Jin, and J. Sun, "De-anonymization of mobility trajectories: Dissecting the gaps between theory and practice," in *Proc. Netw. Distrib. Syst. Secur. Symp.* San Diego, CA, USA: Internet Society, 2018, pp. 1–15. Accessed: Nov. 13, 2022, doi: 10.14722/ndss.2018.23211.

[154] E. Yilmaz, H. Ferhatosmanoglu, E. Ayday, and R. C. Aksoy, "Privacy-preserving aggregate queries for optimal location selection," *IEEE Trans. Depend. Sec. Comput.*, vol. 16, no. 2, pp. 329–343, Mar. 2019, doi: 10.1109/TDSC.2017.2693986.

[155] Y. Pu, J. Luo, Y. Wang, C. Hu, Y. Huo, and J. Zhang, "Privacy preserving scheme for location based services using cryptographic approach," in *Proc. IEEE Symp. Privacy-Aware Comput. (PAC)*, Sep. 2018, pp. 125–126, doi: 10.1109/PAC.2018.00022.

[156] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019, doi: 10.1109/JIOT.2019.2904303.

[157] T. He, E. N. Ciftcioglu, S. Wang, and K. S. Chan, "Location privacy in mobile edge clouds: A chaff-based approach," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2625–2636, Nov. 2017, doi: 10.1109/JSAC.2017.2760179.

[158] C. Gutiérrez-Soto, P. Galdames, C. Faúndez, and C. Durán-Faúndez, "Location-query-privacy and safety cloaking schemes for continuous location-based services," *Mobile Inf. Syst.*, vol. 2022, pp. 1–22, May 2022, doi: 10.1155/2022/5191041.

[159] X. He, J. Liu, R. Jin, and H. Dai, "Privacy-aware offloading in mobile-edge computing," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6, doi: 10.1109/GLOCOM.2017.8253985.

[160] J. Chi, E. Owusu, X. Yin, T. Yu, W. Chan, Y. Liu, H. Liu, J. Chen, S. Sim, V. Iyengar, P. Tague, and Y. Tian, "Privacy partition: A privacy-preserving framework for deep neural networks in edge networks," in *Proc. IEEE/ACM Symp. Edge Comput. (SEC)*, Oct. 2018, pp. 378–380, doi: 10.1109/SEC.2018.00049.

[161] X. Li, S. Liu, F. Wu, S. Kumari, and J. J. P. C. Rodrigues, "Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4755–4763, Jun. 2019, doi: 10.1109/JIOT.2018.2874473.

[162] J. Kim, D. Kim, and S. Choi, "3GPP SA2 architecture and functions for 5G mobile communication system," *ICT Exp.*, vol. 3, no. 1, pp. 1–8, Mar. 2017. Accessed: Nov. 13, 2022, doi: 10.1016/j.icte.2017.03.007.

[163] M. A. Adedoyin and O. E. Falowo, "Combination of ultra-dense networks and other 5G enabling technologies: A survey," *IEEE Access*, vol. 8, pp. 22893–22932, 2020, doi: 10.1109/ACCESS.2020.2969980.

[164] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally, and M. A. Javed, "A survey of device-to-device communications: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2133–2168, 3rd Quart., 2018, doi: 10.1109/COMST.2018.2828120.

[165] O. N. Hamoud, T. Kenaza, and Y. Challal, "Security in device-to-device communications: A survey," *IET Netw.*, vol. 7, no. 1, pp. 14–22, Jan. 2018. Accessed: Nov. 13, 2022, doi: 10.1049/iet-net.2017.0119.

[166] J. Zhang, H. Du, Q. Sun, B. Ai, and D. W. K. Ng, "Physical layer security enhancement with reconfigurable intelligent surface-aided networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3480–3495, 2021, doi: 10.1109/TIFS.2021.3083409.

[167] A. Rahman, E. Hassanain, and M. S. Hossain, "Towards a secure mobile edge computing framework for Hajj," *IEEE Access*, vol. 5, pp. 11768–11781, 2017, doi: 10.1109/ACCESS.2017.2716782.

[168] K. Xiao, W. Li, M. Kadoch, and C. Li, "On the secrecy capacity of 5G mmWave small cell networks," *IEEE Wireless Commun.*, vol. 25, no. 4, pp. 47–51, Aug. 2018, doi: 10.1109/MWC.2018.1700383.

[169] P. Hao, X. Wang, and W. Shen, "A collaborative PHY-aided technique for end-to-end IoT device authentication," *IEEE Access*, vol. 6, pp. 42279–42293, 2018, doi: 10.1109/ACCESS.2018.2859781.

[170] B. Krupp, N. Sridhar, and W. Zhao, "SPE: Security and privacy enhancement framework for mobile devices," *IEEE Trans. Depend. Sec. Comput.*, vol. 14, no. 4, pp. 433–446, Jul. 2017, doi: 10.1109/TDSC.2015.2465965.

[171] X. Wang, Q. Zhou, J. Harer, G. Brown, S. Qiu, Z. Dou, C. Aguayo Gonzalez, A. Hinton, J. Wang, and P. Chin, "Deep learning-based classification and anomaly detection of side-channel signals," in *Proc. Cyber Sens.*, May 2018, pp. 37–44, doi: 10.1117/12.2311329.

[172] C.-L. Chen, M.-L. Chiang, H.-C. Hsieh, C.-C. Liu, and Y.-Y. Deng, "A lightweight mutual authentication with wearable device in location-based mobile edge computing," *Wireless Pers. Commun.*, vol. 113, no. 1, pp. 575–598, Jul. 2020, doi: 10.1007/s11277-020-07240-2.

[173] P. Yu, J. Cao, M. Ma, H. Li, B. Niu, and F. Li, "Quantum-resistance authentication and data transmission scheme for NB-IoT in 3GPP 5G networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–7, doi: 10.1109/WCNC.2019.8885686.

[174] Y. Gao, S. F. Al-Sarawi, and D. Abbott, "Physical unclonable functions," *Nature Electron.*, vol. 3, no. 2, pp. 81–91, Feb. 2020, doi: 10.1038/s41928-020-0372-5.

[175] R. D. Sala, D. Bellizia, and G. Scotti, "A novel ultra-compact FPGA PUF: The DD-PUF," *Cryptography*, vol. 5, no. 3, p. 23, Sep. 2021, doi: 10.3390/cryptography5030023.

[176] J. Zhang, X. Tan, X. Wang, A. Yan, and Z. Qin, "T2FA: Transparent two-factor authentication," *IEEE Access*, vol. 6, pp. 32677–32686, 2018, doi: 10.1109/ACCESS.2018.2844548.

[177] M. Sabbagh, Y. Fei, T. Wahl, and A. A. Ding, "SCADET: A side-channel attack detection tool for tracking prime-probe," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*. San Diego, CA, USA: IEEE Press, Nov. 2018, pp. 1–8. Accessed: Nov. 14, 2022, doi: 10.1145/3240765.3240844.

[178] M. Mushtaq, A. Akram, M. K. Bhatti, R. N. B. Rais, V. Lapotre, and G. Gogniat, "Run-time detection of prime + probe side-channel attack on AES encryption algorithm," in *Proc. Global Inf. Infrastruct. Netw. Symp. (GIIS)*, Oct. 2018, pp. 1–5, doi: 10.1109/GIIS.2018.8635767.

[179] X. Yang, Y. Zhang, S. Wang, B. Yu, F. Li, Y. Li, and W. Yan, "LedgerDB: A centralized ledger database for universal audit and verification," *Proc. VLDB Endowment*, vol. 13, no. 12, pp. 3138–3151, Aug. 2020. Accessed: Jun. 9, 2023, doi: 10.14778/3415478.3415540.

[180] C. Yue, T. T. A. Dinh, Z. Xie, M. Zhang, G. Chen, B. C. Ooi, and X. Xiao, "GlassDB: An efficient verifiable ledger database system through transparency," *Proc. VLDB Endowment*, vol. 16, no. 6, pp. 1359–1371, Feb. 2023. Accessed: Jun. 9, 2023, doi: 10.14778/3583140.3583152.

[181] P. Antonopoulos, R. Kaushik, H. Kodavalla, S. Rosales Aceves, R. Wong, J. Anderson, and J. Szymaszek, "SQL ledger: Cryptographically verifiable data in azure SQL database," in *Proc. Int. Conf. Manage. Data*. New York, NY, USA: Association for Computing Machinery, Jun. 2021, pp. 2437–2449. Accessed: Jun. 9, 2023, doi: 10.1145/3448016.3457558.

[182] A. Pathak, I. Al-Anbagi, and H. J. Hamilton, "TABI: Trust-based ABAC mechanism for edge-IoT using blockchain technology," *IEEE Access*, vol. 11, pp. 36379–36398, 2023, doi: 10.1109/ACCESS.2023.3265349.

[183] M. J. Amiri, T. Allard, D. Agrawal, and A. E. Abbadi, "PReVer: Towards private regulated verified data," in *Proc. 25th Int. Conf. Extending Database Technol. (EDBT)*, Apr. 2022, pp. 1–8. Accessed: Jun. 9, 2023, doi: 10.48786/edbt.2022.40.

[184] D. L. Fekete and A. Kiss, "A survey of ledger technology-based databases," *Future Internet*, vol. 13, no. 8, p. 197, Jul. 2021. Accessed: Jun. 9, 2023, doi: 10.3390/fi13080197.

[185] S. Lupaiescu, P. Cioata, C. E. Turcu, O. Gherman, C. O. Turcu, and G. Paslaru, "Centralized vs. Decentralized: Performance comparison between BigchainDB and Amazon QLDB," *Appl. Sci.*, vol. 13, no. 1, p. 499, Dec. 2022. Accessed: Jun. 9, 2023, doi: 10.3390/app13010499.

[186] X. Yang, S. Wang, F. Li, Y. Zhang, W. Yan, F. Gai, B. Yu, L. Feng, Q. Gao, and Y. Li, "Ubiquitous verification in centralized ledger database," in *Proc. IEEE 38th Int. Conf. Data Eng. (ICDE)*, May 2022, pp. 1808–1821, doi: 10.1109/ICDE53745.2022.00181.

SAMSON O. ORUMA received the bachelor's degree in electrical and electronics engineering from the University of Benin, Benin City, Nigeria, and the master's degree in information and communication engineering from Covenant University Ota, Ogun State, Nigeria. He is currently pursuing the Ph.D. degree with the Institute for Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU), Gjøvik, Norway. He is a Ph.D. Research Fellow with Østfold University College, Halden, Norway. He is also a member of the Nigerian Society of Engineers (NSE) and the SecuRoPS Project in Norway. His research interest includes developing a user-centered security framework for social robots in public spaces.

SLOBODAN PETROVIĆ received the Ph.D. degree from the University of Belgrade, Serbia, in 1994. From 1986 to 2000, he was with the Institute of Applied Mathematics and Electronics and the Institute of Mathematics, Belgrade. From 2000 to 2004, he was involved in various information security-related projects with the Institute of Applied Physics, Madrid, Spain. From 2004 to 2015, he was with Gjøvik University College, Norway. Since January 2016, he has been a Professor of information security with the Norwegian University of Science and Technology (NTNU), where he teaches cryptology and intrusion detection and prevention. He is the author of more than 50 scientific papers from the field of information security, digital forensics, and cryptology. His research interests include cryptology, intrusion detection, and digital forensics.