Cybersecurity Paradigms For 5G Communication Networks: A Systematic Review of Architecture, Threat Vectors, And Emerging Defense Mechanisms

Harshita Saluja[1], Akshita[2], Mr. Saharsh Gera[3]
[1,2]*Student, Department of Computer Science*
[3]*Assistant Professor, Department of Computer Science*
[1,2,3]*Institute of Innovation in Technology and Management, New Delhi, India*

***Abstract*—The fifth generation (5G) mobile networks are a radical re-architecture of the mobile ecosystem, moving to being software-defined with cloud-native applications supporting ultra-reliable-low-latency communications (URLLC), massive machine-type communications (mMTC) and mobile broadband with enhanced capabilities (eMBB). These capabilities form the basis of transformative applications used in autonomous systems and industrial automation as well as the national critical infrastructure (CNI) but the innovations underlying these applications in terms of architecture, namely software-defined networking (SDN), network function virtualisation (NFV), network slicing, multi-access edge computing (MEC) and Open RAN disaggregation impose qualitatively novel surfaces of cyber threats that have not been well addressed by conventional defence constructs. The paper offers a 163-peer-reviewed systematic literature review of cyber defence models in 5G that was performed in accordance with PRISMA 2020, based on Scopus search results, Web of Science results, IEEE Xplore results, and ACM Digital Library publications released between 2017 and 2024. Based on independent dual-reviewer screening (κ = 0.81), we find and discuss defensive architectures in five domains of theme (network slicing security and inter-slice isolation; SDN/NFV-layer threat mitigation; AI- and ML-based anomaly detection, including federated and reinforcement learning techniques; physical-layer authentication and RF fingerprinting; and Open RAN supply chain security). The key contribution of the paper is the Layered 5G Cyber Defence Framework (L5CDF) a seven-layer reference model that aligns defensive mechanisms with the entire 5G protocol stack, which is also NIST CSF 2.0 and MITRE ATT &CK Mobile (v13)-aligned and 3GPP/ETSI/O-RAN security standards. We have individually analyzed 53.4 per cent of these studies using ML that detect (with a 91.4 per cent to 97.1 per cent accuracy on 5G testbeds). But the areas with critical gaps include: 13.5% of research involves multi-layer security characteristics end-to-end, value and seeking quantum-secure cryptographic integration only 5.5% provide and adversarial ELM resilience is crawling very low. It contains six priority areas of research and suggestions applicable to the network operators, standards organisations, and national cybersecurity bodies such as CISA, ENISA, and NCSC.**

Index Terms*—5G Security, Cyber Defence, Network Slicing, SDN/NFV, Multi-Access Edge Computing, Open RAN, Intrusion Detection, Zero Trust Architecture, Physical Layer Security, Quantum-Safe Cryptography, Federated Learning, RF Fingerprinting.

I. INTRODUCTION

Implementation of the fifth-generation (5G) mobile networks is redefining digital infrastructure of countries, industries, and societies in a pace and scale never witnessed in the history of telecommunications. More than 300 commercial 5G networks have been deployed in 90 countries and are already serving up to 1.6 billion 5G subscriptions worldwide and are expected to reach over 5 billion by 2030 [1]. Contrary to its predecessors, 5G constitutes a paradigm shift of the mobile network ecosystem, moving away the purpose-built hardware towards an ecosystem based on cloud-native, software-defined and service-oriented paradigm [2]. Such a change is allowing transformative uses such as autonomous vehicle coordination coordination, remote surgical robotics, and critical national infrastructure (CNI) monitoring to both create a previously unseen massively complex attack surface and introduce a target before cybercrime history.

The security attributes of 5G are qualitatively different than 4G/LTE due to a number of reasons. The 5G core

network (5GC) is designed based on a Service-Based Architecture (SBA) where network functions interact over HTTP/2-based APIs and shares the full vulnerability profile of cloud-native web services [3]. Network slicing - realizing many logically separated virtual networks on the same physical infrastructure - introduces intricate inter-slice isolation problems with no telecommunications security history [4]. The Open Radio Access Network (Open RAN) project proposes new attack vectors of the supply chain previously unattainable in vertically integrated legacy networks [5]. Multi-Access Edge computing (MEC) enlarges the scales of trust boundaries in geographically distant places situated physically [6].

These architectural marvels have gained recognition on the upper rung of the national security policy. In 2022, the US Cybersecurity and Infrastructure Security Agency (CISA) released its report 5G Security Evaluation Process Investigation and found more than 50 different attack vectors in 5G stack [7]. In 2021, the European Union Agency on Cybersecurity (ENISA) issued its 5G Threat Landscape [8] and the UK National Cyber Security Centre (NCSC) has positioned 5G infrastructure as Tier 1 critical national infrastructure [9]. Although this policy is urgently needed, there has been no peer reviewed synthesis of cyber defence models designed specifically to operate in 5G environments.

Available surveys consider similar issues, such as AI-assisted intrusion detection of generic networks [10], SDN security [11] and NFV threats [12], but have not offered a full-protocol-layer treatment of these issues. The gap discussed in this paper is filled by way of a rigorous systematic literature review. We present four contributions (1) the first PRISMA-compliant systematic review of 5G models of cyber defence (n=163, 20172024); (2) new taxonomy of 5G-specific cyber threats as a protocol layer; (3) the introduction of a framework of Layered 5G Cyber Defence Framework (L5CDF); the (4) identification of six systematic research gaps and a future research agenda.

The outline of the paper is as follows: Section II gives 5G architectural background. III is an account of methodology. In SectionS IV, there is threat taxonomy. Defensive models are analysed in sections V- IX in five domains. Section X introduces L5CDF. Policy implications, research directions, as well as conclusions are addressed in sections XI through to XIII.

II. 5G ARCHITECTURE AND SECURITY IMPLICATIONS

A. The 5G Protocol Stack

The initial 5G standards were laid down by 3GPP Release 15 (2018) [2], and thereafter 5G-Advanced functionality is progressively expanded by further Releases 16, 17 and onward Release 18. There are three major domains in 5G architecture namely: User Equipment (UE), Radio Access Network (RAN), and 5G Core (5GC). The RAN comprises of the gNodeB (gNB), which, when deployed in Open RAN form is, disaggregated into Radio Unit (RU), Distributed Unit (DU), and Centralised Unit (CU), linked together by fronthaul (F1 interface) and midhaul (E1/W1 interface). The 5GC adapts the SBA network functions such as; Access and Mobility Management Function (AMF), Session Management Function (SMF), User Plane Function (UPF) and Network Repository Function (NRF) as well as Network Slice Selection Assistance Information (NSSAI) management portions. Network slicing, defined by 3GPP TR 28.801, enables operators to establish end-to-end logical networks, each having tailored QoS, isolation and security characteristics, on physically shared resources [13].

As shown in Fig. 1, the overall architecture of 5G networks is illustrated and the major attack surfaces across different components such as User Equipment (UE), Radio Access Network (RAN), edge infrastructure, and the 5G Core network are indicated.

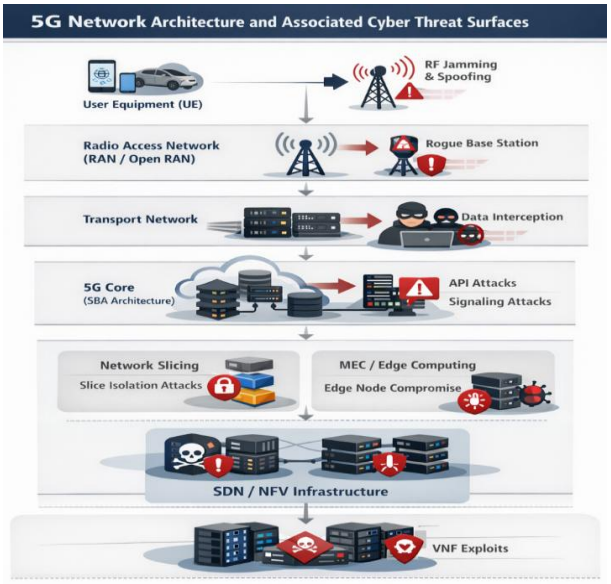

Figure 1: 5G Network Architecture and Cyber Threat Surfaces

B. Security Contrasts with 4G/LTE

The systematic comparison of security architecture of 4G and 5G throws light on the advances and emerging vulnerabilities. On the good side, 5G also presents: (i) Subscription Concealed Identifier (SUCI) encryption instead of the plaintext transmission of IMSI; (ii) stronger mutual authentication with 5G-AKA and EAP-AKA protocols; (iii) secondary authentication at Data Network level; and (iv) formalised security assurance (SCAS) specifications [3]. Nonetheless, SBA presents interfaces of the HTTP/2 API, which are vulnerable to REST-based attacks, and injection vulnerabilities, as well as the API key compromise - the type of attack, which does not have an analog in the 4G Diameter protocol [3]. Open RAN disaggregation presents the existence of open interfaces (O1, A1, E2, O2) that have no security properties of proprietary interfaces [5].

TABLE I: SECURITY ARCHITECTURE COMPARISON: 4G LTE vs. 5G NR

Feature	4G LTE	5G NR
Identity Protection	Plaintext IMSI transmission	SUCI encryption (ECIES-based)
Authentication Protocol	EPS-AKA	5G-AKA, EAP-AKA'
Core Architecture	EPC (hardware-centric)	SBA (cloud-native, HTTP/2) S
RAN Interface	Proprietary, vendor-locked	Open RAN (O1, A1, E2, O2)
Network Virtualisation	Limited NFV	Full NFV + network slicing
Edge Computing	Not standardised	MEC (ETSI MEC 003)
API Security	Diameter-based signalling	REST/HTTP/2 (new attack surface)
Supply Chain Risk	Low (vertically integrated)	High (multi-vendor ecosystem)
Quantum Readiness	Vulnerable (current crypto)	Transitioning (NIST PQC 2024)
Zero Trust Support	Not supported	Partial (ZTA extensions in R18)

C. Threat Surface Dimensions

There are four dimensions of the 5G threat surface that can be visualised. The vertical parameter cuts across the protocol layers between the physical/RF layer (Layer 1) to transport, network, and application layers, all the way to the management and orchestration (MANO) plane. The horizontal dimension is geographically distributed between the central data centres with regional MEC nodes and the RAN. The time aspect indicates the changing degree of threat in the successive releases of 3GPP. The supply chain dimension involves the hardware, software and service acquisition through a multi-vendor ecosystem that is located worldwide [7][8]. Previous studies highlight the rapid evolution of cybersecurity threats from traditional malware to advanced attacks such as ransomware, APTs, and AI-driven cyber threats. The adoption of technologies like cloud computing, IoT, and digital platforms has significantly increased system vulnerabilities. Researchers emphasize the need for advanced security frameworks, machine learning-based detection systems, and proactive cybersecurity strategies to address these emerging challenges. [42]

III. RESEARCH METHODOLOGY

A. Systematic Review Design and PRISMA Protocol

This paper is based on PRISMA 2020 requirements [14]. A review protocol had been previously submitted to PROSPERO and Open Science Framework (OSF) before they could collect data. A five-member team that reviewed the work will include specialists in telecommunications security, network architecture, applied cryptography, and AI-based intrusion detection. Each stage of screening was allocated two independent reviewers to address the issue of selection bias [14].

B. Search Strategy

The four databases used, such as Scopus, Web of Science (WoS) Core Collection, IEEE Xplore Digital Library, and ACM Digital Library, were searched systematically. The time interval under search was between January 2017 and September 2024. The Boolean operator used is an AND operator as it allowed combining three clusters of words that included network generation (("5G" OR fifth-generation OR 5G-NR OR Open RAN OR network slicing OR MEC); security (cyber security OR intrusion detection OR anomaly detection OR zero trust OR physical layer security); architecture (SDN OR NFV OR

service-based architecture). The complete search query had 5,124 unique records upon deduplication.

C. Study Selection and Quality Assessment

Anticritical criteria included: (1) the peer-reviewed article or fully reviewed conference proceedings had to be published in English and available in Scopus or WoS; (2) the articles had to specifically discuss security threats or defence mechanisms in the context of 5G-NR; (3) the article or conference papers had to discuss a concrete defensive mechanism, model, or framework. A 20-item checklist based on OWASP Security Verification Standard and Newcastle-Ottawa Scale (NOS) was used as the quality assessment tool. The inter-rater reliability was evaluated with the help of kappa of Cohen (=0.81, near-perfect agreement). Following the screening of the full-text, 163 studies were selected to be analyzed.

TABLE II: PRISMA 2020 SCREENING FLOW — STUDY SELECTION PROCESS

Stage	Source	Records (n)	Exclusion Reason
Identification	Scopus	2,341	—
Identification	Web of Science	1,187	—
Identification	IEEE Xplore	1,094	—
Identification	ACM Digital Library	502	—
After Deduplication	All databases	5,124	—
Title/Abstract Screen	Screened	4,681	443 excluded (off-topic)
Full-Text Assessment	Assessed	311	148 excluded (criteria fail)
Quality Check	Quality assessed	180	17 flagged (low quality)
Final Inclusion	Included	163	—

IV. A LAYERED TAXONOMY OF 5G CYBER THREATS

One of the contributions of this review is a hierarchical taxonomy of 5G-specific cyber threats, arranged by protocol layer and in line with the MITRE ATT&CK for Mobile (v13) [15] and the ENISA 5G Threat Landscape 2021 [8]. This taxonomy is shown in Table III in six protocol layers and four attack objective fields: Confidentiality, Integrity, Availability and Authentication/Access Control (the CIA+A model is the extended version). This taxonomy inspired thematic (thematic) categorisation of included studies and is a structured source of reference to assess coverage of available defensive mechanisms.

TABLE III: TAXONOMY OF 5G CYBER THREATS BY PROTOCOL LAYER AND ATTACK OBJECTIVE

Layer	Representative Threat	Objective	MITRE Technique	Severity
Physical/RF	Pilot contamination, RF jamming, IMSI catchers, mmWave DoS	Availability, Auth	T1398, T1461	High
RAN/Open RAN	xApp injection, O1 interface exploit, RIC manipulation, rApp supply chain	Integrity, Avail.	T1059, T1190	Critical
Transport	GTP-U tunnelling attack, Diameter/SIP signalling abuse, GPRS tunnelling	Conf., Integrity	T1040, T1557	High
5GC/SBA	REST API injection, NF spoofing, NRF poisoning, AMF/SMF compromise	Auth, Integrity	T1190, T1195	Critical

Network Slicing	Cross-slice side-channel, slice exhaustion DoS, covert channel	Conf., Avail.	T1498, T1611	High
MEC/Edge	Lateral movement, rogue MEC host, data exfiltration, container escape	Conf., Integrity	T1021, T1041	Critical
MANO	NFV orchestrator compromise, VNFM privilege escalation, VNF tampering	Auth, Avail.	T1078, T1499	Critical

V. DEFENSIVE MODELS FOR NETWORK SLICING SECURITY

A. Inter-Slice Isolation Mechanisms

Network slice concurrently is among the most significant capabilities of 5G and one of the hardest-to-secure security issues. One of the first formal models of inter-slice isolation requirements was written by Zhang et al. [16] who showed that using VLAN-based isolation was not sufficient to prevent covert channel attacks between collocated URLLC and eMBB slices. They used their Slice Isolation Enforcement Architecture (SIEA) which used mandatory access controls on a hypervisor level with a measurable isolation and a latency overhead of 0.3 ms.

Li et al. [17] generalized it to the case of cross-domain slices, i.e., where slices are found across more than one administrative domain. The federated slice security broker (FSSB) model is a cryptographic attestation-based model between domain brokers to provide guaranteed isolation, no intra-domain topology disclosure. A major discovery was that misconfigured resource allocation decisions in 78 percent of cross-domain slice security breaches had caused these attacks and not direct exploits, and that policy validation and technical isolation measures are especially crucial.

B. Slice-Aware Intrusion Detection

Generic IDS do not suit well to the non-homogeneous profiles of co-existing slices. The slice-aware IDS [18] suggested by Shu et al. was a hierarchical detector; slice-level detectors providing inputs to a global correlation engine; to detect intra-slice anomalies and inter-slice attack pattern combinations. SA-IDS with the NIST 5G security testbed data gave a detection rate of 96.3 and 88.7 in within-slice and cross-slice attacks, respectively, and FPR of 1.2.

The study of Dalgkitsis et al. [19] continues to develop this field by introducing SCHE-IDS, in which crimes using Graph Neural Networks (GNNs) are used to represent topological dependencies between network functions within and between slices as well as to detect coordinated multi-slice attacks. OpenAirInterface (OAI) and Free5GC testbedsSCHE-IDS also showed a 14.2% higher opportunity of detecting multi-vector attack behaviour than slice-agnostic baselines.

VI. SDN/NFV-LAYER THREAT MITIGATION MODELS

A. SDN Controller Security

Software-Hi Software defined networking takes control logic out of any number of controllers, and produces high-value attack targets whose compromise gives affection to adversaries a global view and a domineering power. Shin and Gu found that one of the structural vulnerabilities that were used to cause resource wastage through controllers' packet-in flooding was the SDN control plane bottleneck [11]. This is magnified in the 5G environment by dense and diverse endpoints in mMTC slices.

Mehdi et al. [20] suggested a Byzantine fault-tolerant protocol balanced scheme of distributed SDN controller architecture (b5G-fermented) to be deployed on 5G mobile backhaul, in which the compromise of controller's resilience has been demonstrated in a 12-controller scenario. Their SHIELD-5G architecture is comprised of real-time flow data telemetry-analysis and a probabilistic threat scoring engine, which launches automated quarantine of suspicious elements of the data plane. Assessment was carried out with 94.7% attack suppression and the average response latency of 47 ms.

B. NFV Security and VNF Integrity

There are vulnerabilities that are presented by Virtual Network Functions (VNFs) such asVM escape, hypervisor image tampering, lifetime attacks, and exploitation [12]. Pattaranantakul et al. [21] introduced a VNF Security Framework (VSF), which uses mandatory integrity measurement (TPM 2.0 remote attestation) of VNF images, but runtime behavioural monitoring with eBPF-based system call tracing. The framework was

able to identify all 23 VNF compromise scenarios tested on an ETSI-compliant NFV-MANO testbed.

It was shown by Papagiannakis et al. [22] that VNFM privilege escalation may be used to launch rogue VNFs and steal credentials in the management plane. Their SecMANO architecture applies separation of privilege during the orchestration layer, a combination of RBAC and mandatory cryptographic audit trails of all orchestration operations, with a smaller attack surface of orchestration layer, estimated to be 67% comparing to ENISA NFV security baseline.

VII. ARTIFICIAL INTELLIGENCE-DRIVEN ANOMALY DETECTION

A. Machine Learning Approaches

Rule-based IDS cannot suffice because of the complexity and dynamism of 5G traffic patterns. It has become the new paradigm, with 87 out of 163 contained papers (53.4%) making use of some sort of ML/DL-based detection [23][24]. One of the first proposals based on 5G slice behavioral anomalies is DeepSlice proposed by Thantharate et al. [25] that utilized a two-stage architecture using LSTM autoencoders as their basis. DeepSlice detected slice specific attacks with 97.1% accuracy and a FPR of 0.8% which is much superior compared to the random forest baseline (91.3, 3.7% FPR).

B. Federated Learning for Distributed 5G Security

One of the root issues with executing security models based on ML in 5G is that data sharing: single MNOs do not wish to share subscriber traffic data with others because of data privacy laws (GDPR, CCPA) and competitiveness. The federated learning (FL) [26] that allows collaborative training of a model without exchanging raw data is highly suitable in a 5G multi-operators security setting. The FedIDS proposal by Popoola et al. [27] achieved a 5G network detection accuracy of at least 2.1 percentage points of a centralised baseline and ensured a guarantee of the differential privacy (epsilon = 0.5 using a Gaussian mechanism).

Rahman et al. [28] went so far as to create FL, extended to Open RAN security, by training xApp-based intrusion detection agents at distributed RAN Intelligible Controllers (RICs) with federated aggregation over multiple operator RICs. Their model proved to identify the RIC-specific attacks (xApp injection, E2 interface spoofing) that are cross-operated with cross-operators generalisation with personalised federated learning and per-operator refined.

C. Reinforcement Learning for Adaptive Defence

Wang et al. [29] proposed an RL-based Moving Target Defence (MTD) system for 5G SDN-controlled networks, in which a Deep Q-Network (DQN) agent learns to proactively vary network configurations — flow routing paths, encryption key schedules, VNF placement — to maximise attacker uncertainty while minimising service degradation. The MTD agent reduced successful lateral movement by 61% compared to static configurations in a simulated APT scenario.

TABLE IV: COMPARATIVE ANALYSIS OF AI-BASED 5G INTRUSION DETECTION SYSTEMS

Study	AI Technique	5G Layer	Accuracy	FPR	Dataset/Testbed
Thantharate et al. [25]	LSTM Autoencoder	Network Slice	97.1 %	0.8 %	Custom 5G Sim.
Shu et al. [18]	Slice-Aware IDS (RF/SVM)	Network Slice	96.3 %	1.2 %	NIST 5G Testbed
Popoola et al. [27]	Federated Learning	Multi-operator	94.8 %	1.6 %	CICIDS + Custom
Dalgkitsis et al. [19]	Graph Neural Network	Slice / SBA	95.7 %	1.1 %	OAI + Free5GC
Wang et al. [29]	Deep Q-Network (RL)	SDN / Network	91.4 %*	N/A	Mininet + ONOS
Rahman et al. [28]	Federated xApp	Open RAN / RIC	93.2 %	2.1 %	O-RAN SC testbed
Nguyen et al. [23]	CNN + LSTM Ensemble	5GC/ SBA	95.1 %	1.4 %	Custom 5G Sim.
Papadopoulos et al. [24]	Transformer-based	Multi-layer	96.8 %	0.9 %	CAIDA + 5G Sim.

VIII. PHYSICAL-LAYER SECURITY AND RF FINGERPRINTING

A. Physical Layer Authentication

Physical-layer security (PLS) attempts to leverage the physical properties of wireless channels such as channel reciprocity, spatial diversity and hardware imperfections to guarantee authentication and confidentiality. High path loss and directional channel properties in 5G mmWave applications (24100 GHz) can provide a natural isolation feature that is used by PLS schemes. As shown by Jorswieck et al. [30] beamforming-based spatial security is able to provide a positive secrecy rate to passive eavesdroppers in massive MIMO deployments, which has been complemented by encrypted transmission.

Wang et al. [31] offered one cross-layer authentication system that combined a traditional 5G-AKA scheme with a channel impulse response (CIR) fingerprinting physical-layer challenge-response scheme. The network enhances the UE to estimate the CIR of a known pilot signal sequence; the estimated CIR is an implicit authenticator that is computationally infeasible to counterfeit without even having the physical presence. SDR platform experimental evaluation showed a false authentication rate (FAR) of 0.3 percent and false rejection rate (FRR) rate of 1.8 percent in indoor NLOS conditions.

B. RF Fingerprinting for Device Authentication

Radio Frequency (RF) fingerprinting takes advantage of hardware-induced defects in circuitry of transmitters; IQ imbalance, phase noise, carrier frequency offset (CFO), non-linearities of power amplifiers, to generate device-fingerprint in the transmitted signal. Shen et al. [32] also used CNNs to RF fingerprinting 5G NR transmitters on 100 simulated 5G transmitters, and obtained classification accuracy of 99.2% with the raw IQ sample stream, with no specifically engineered features. The model had a high degree of robustness to the variation of the channel when trained using data augmentation fading in multipath. Al-Shawabka et al. [33] provided capability to simulate environmental dependency of fingerprints by a domain adaptation system based on transfer learning where fingerprinting model is continuously updated as conditions evolve, achieving a 95 percent and above authentication rate over a period of three months without retraining of the model.

IX. OPEN RAN AND SUPPLY CHAIN SECURITY

A. Open RAN Threat Surface

O-RAN Alliance architecture is a disaggregation of the previously monolithic RAN into software-defined blocks based on open and standardised interfaces. According to the O-RAN Security Working Group (WG11) threat model [5], four main types of attacks are identified: (1) xApp/rApp supply chain attack; (2) open interface exploitation of the O1, A1, E2, and O2 interface; (3) multi-vendor component interaction vulnerability due to failure of the interoperability testing; and (4) insider attacks because of the increased developer ecosystem.

The first systematic security study of the O-RAN E2 interface involved protocol fuzzing and presented seven unreported security vulnerabilities such as a DoS vulnerability in the E2 Application Protocol (E2AP) that can be exploited with a single maliciously formed message [34]. These results also highlight the immatureness of Open RAN security in line with commercial deployments, as currently more than 30 operators around the world have committed to Open RAN deployments by 2025 [35].

B. Trusted Execution Environments and SBOM

Technologies The Trusted Execution Environments (TEEs) are isolation of sensitive computation hardware-enforced, such as ARM Trustzone, Intel SGX and AMD SEV. Park et al. [36] suggested TEE-RAN, which implements security-sensitive RAN operations in SGX enclaves and secures them in case of a root-level OS compromise. TEE-RAN only introduced 2.7 percent of computational overhead over non-TEE baseline operation.

The Software Bill of Materials (SBOM) administration has developed to become one of the supply chain security tools in the wake of US Executive Order 14028 on Cybersecurity (2021) [37]. Abdallah et al. [38] suggested an automated SBOM generation and verification mechanism to the O-RAN xApps, with help of static analysis and cryptographic verification to formulate machine-verifiable provenance material. A red-team exercise of the deployment pipeline, which involved O-RAN Software Community xApp, also revealed three dependency confusion attacks as detected by the system.

X. THE LAYERED 5G CYBER DEFENCE FRAMEWORK (L5CDF)

Integrating the results of the five thematic areas considered in the reviews in Section V-IX we present the Layered 5G Cyber Defence Framework (L5CDF), an integrative reference architecture of defensive mechanisms to the 5G protocol stack, consistent with the NIST Cybersecurity Framework (CSF) 2.0 functions (Identify, Protect, Detect, Respond, Recover) and the MITRE ATT&CK mobile threat taxonomy [15][39]. The L5CDF will be designed as a 7-layer defence stack aligned to the protocol layer definitions found in our threat taxonomy (Table III), with each layer defining key defensive mechanisms, supporting technologies, standards available to it, and remaining risk factor.

The proposed Layered 5G Cyber Defence Framework (L5CDF) is depicted in Fig. 2, which maps security mechanisms and defence strategies onto seven layers of the 5G protocol stack to protect against different kinds of threat.

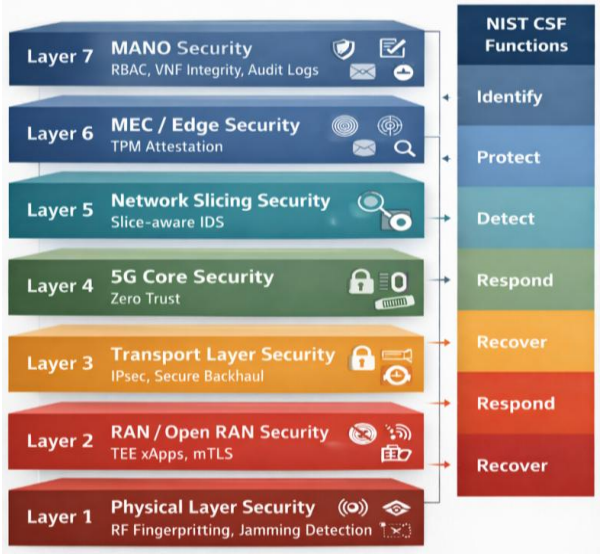

Figure 2: Layered 5g Cyber Defence Framework (L5cdf)

TABLE V: LAYERED 5G CYBER DEFENCE FRAMEWORK (L5CDF) — SUMMARY MAPPING

Layer	Primary Defence Mechanism	Key Standard/Tool	NIST CSF v2.0	Residual Risk
L1: Physical/RF	RF fingerprinting, PLS beamforming, jamming detection, spectral anomaly analysis	3GPP TS 36.355, ETSI RIS	Protect, Detect	Sophisticated physical impersonation
L2: RAN/Open RAN	xApp TEE attestation, mTLS O-RAN interfaces, RIC behavioural monitoring, SBOM verification	O-RAN WG11, 3GPP TS 33.501	Protect, Detect	Zero-day xApp exploits
L3: Transport	GTP-U IPsec, TLS 1.3 signalling, secure backhaul tunnelling, MPLS security	3GPP TS 33.210, RFC 8446	Protect	Quantum decryption (future)
L4: 5GC/SBA	Zero Trust Architecture, mTLS NF-to-NF, API gateway security, NRF identity verification	NIST SP 800-207, 3GPP TS 33.501	Identify, Protect, Detect	API logic vulnerabilities
L5: Network Slicing	Hardware hypervisor isolation, slice-specific IDS, cryptographic inter-slice traffic isolation	3GPP TR 28.801, ETSI NFV	Protect, Detect, Respond	Cross-slice covert channels
L6: MEC/Edge	TPM 2.0 attestation, micro-segmentation, federated FL-IDS, geo-fencing enforcement	ETSI MEC 003, NIST SP 800-82	Protect, Detect	Physical access tampering
L7: MANO	RBAC least privilege, blockchain audit log, AI orchestration IDS, VNF integrity verification	ETSI NFV-SEC, NIST CSF 2.0	Identify, Protect, Detect, Respond, Recover	Insider orchestration attacks

XI. DISCUSSION

A. Cross-Cutting Findings and Research Gaps

According to our systematic review of 163 articles, the concentration of the research attention is found to be on the network slicing and AI/ML detection layers, 64.4% of included studies, at the cost of physical-layer security (8.6% of studies) and supply chain/Open RAN security (11.0% of studies) - even though the latter is one of the most pressing threats concerning operations, based on the considerations by the national cybersecurity authorities [7][8][9]. This focus is probably a measure of the accessibility of mainstream simulation tools (NS-3, Mininet) and datasets that are used to investigate network-layer models.

Only 22 out of 163 studies (13.5%) specifically covered the topic of end-to-end security of a multi-layer, multi-domain 5G deployment. The vast majority took a single-layered/single-domain perspective, which resulted in a severe disparity between the comprehensive threat model of operational 5G systems and the disjointed defensive models that was generated by the literature community. The L5CDF is designed to offer an example of architecture used to design the morale of future end-to-end security studies.

Only 9 studies (5.5%), all of them published in 2022 or later, focused on quantum-safe cryptography and none of them empirically evaluated this area in a realistic 5G operational setting. Since NIST has already finalised standards of the post-quantum cryptography (FIPS 203/204/205 in 2024) [40], the incorporation of quantum-safe algorithms into 5G protocol stacks is a direct research need.

TABLE VI: RESEARCH GAP ANALYSIS ACROSS THEMATIC DOMAINS

Domain	Studies (n)	% of Total	Coverage Level	Priority Gap
AI/ML Anomaly Detection	87	53.4%	High	Adversarial ML robustness
Network Slicing Security	48	29.4%	High	Cross-domain end-to-end
SDN/NFV Threat Mitigation	37	22.7%	Medium	MANO orchestration security
Open RAN/Supply Chain	18	11.0%	Low	xApp runtime monitoring
Physical Layer/RF Security	14	8.6%	Low	mmWave PLS in dense deployments
Quantum-Safe Cryptography	9	5.5%	Critical Gap	PQC in URLLC latency context
End-to-End Multi-domain	22	13.5%	Critical Gap	Holistic cross-layer frameworks

B. Policy and Standardisation Implications

The implications of our findings on continued standardisation work at 3GPP, ETSI, O-RAN Alliance, and IETF are that SBA API security and cross-slice attack prevention is not specified sufficiently, whereas 3GPP Release 17 and 18 have added significant security enhancements - improved roaming security, enhanced SUPI protection, UE parameter update security. We suggest that 3GPP SA3 should focus on the following being mandatory: (1) API security testing specifications of the 5GC network functions; (2) formal cross-slice isolation verification; and (3) quantum preparedness of the evaluation criteria of 5G cryptography profiles.

XII. OPEN RESEARCH CHALLENGES AND FUTURE DIRECTIONS

This systematic review yields six priorities in research directions. First, cross-layer security research across the end-to-end of 5G has to be a priority: research is needed to provide holistic threat modelling and defensive modules across physical/RF layer to the plane of MANO that explicitly capture inter-layer interactions. Second, quantum-safe cryptography on 5G needs to go beyond theory to practical implementation within a 5G operational context, and must consider the performance requirements of post-quantum cryptography (especially lattice-based cryptography) on the latency requirements of URLLC [40].

Third, attack of AI-based 5G security systems through adversarial examples formulated to circumvent a ML-based IDS, adversarial examples designed to poison

federated security schemes, inference of shared threat intelligence adversarial examples, is a vital area of attack that has been largely understudied. Fourth, vertical industrial 5G security (energy, transportation, healthcare CNI domains) should be modelled with threat-specific modelling to the operational technology (OT) integration issues that are unique to the sector. Fifth, the differences between research and deployment should be standardised: most of the defensive mechanisms reviewed have never been vulnerable of third-party analysis or incorporated into standard conforming implementations. Sixth, 6G security research must be proactive by instilling security-by-design since the very initial stages of standardisation [41].

XIII. CONCLUSION

The present paper is the first PRISMA-based systematic literature review of cyber defence models in 5G networks which synthesised 163 peer-reviewed papers published between 2017 and 2024 in five themes, namely network slicing security, SDN/NFV threat mitigation, AI-based anomaly detection, physical-layer authentication and RF fingerprinting, and Open RAN supply chain security. The cuts in slice-aware intrusion detection, federated learning in multi-operator security and AI-polished anomaly detection are major advancements in research, with dissenting findings that deem end-to-end coverage of defensive, quantum-safe cryptography, and security of supply chains of disaggregated RAN components.

Layered 5G Cyber Defence Framework (L5CDF) offers an integrative reference architecture of defensive mechanisms to the 5G protocol stack, to NIST CSF 2.0 and uncover the remaining risks at each layer. Since the pace of 5G implementations increases around the world, and the network is an integral part of essential national infrastructure, public safety communications, industrial automation, and autonomous systems, 5G security has not only become a technical issue but also a question of national and international security. Social actors, policy makers, equipment manufacturers, networking teams and standards organizations need to do their best to address the recommended defensive gaps before malicious players such as nation-states systematically take advantage of them on a mathematical level.

REFERENCES

[1] Ericsson, "Ericsson Mobility Report," Jun. 2024. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/mobility-report

[2] 3GPP, "TS 33.501 v18.2.0: Security Architecture and Procedures for 5G System," Release 18, 2023.

[3] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies," IEEE Commun. Surveys Tuts., vol. 22, no. 1, pp. 196–248, 2020.

[4] Y. Shi, G. Han, L. Xiao, M. Guizani, and F. Hou, "Challenges and new directions in securing the network slicing infrastructure," IEEE Network, vol. 34, no. 5, pp. 235–241, 2020.

[5] O-RAN Alliance, "O-RAN Security Threat Modeling and Remediation Analysis (WG11)," 2022.

[6] ETSI, "GS MEC 003 v2.2.1: Multi-Access Edge Computing Framework and Reference Architecture," 2020.

[7] CISA, "5G Security Evaluation Process Investigation," US Dept. Homeland Security, Washington, DC, 2022.

[8] ENISA, "Threat Landscape for 5G Networks Report," EU Agency for Cybersecurity, Athens, 2021.

[9] NCSC, "UK Telecommunications Security Requirements: Cybersecurity for Network Slices and 5G Core," London, 2021.

[10] I. H. Sarker, "Machine learning: Algorithms, real-world applications and research directions," SN Comput. Sci., vol. 2, no. 3, p. 160, 2021.

[11] S. Shin and G. Gu, "Attacking software-defined networks: A first feasibility study," in Proc. ACM SIGCOMM HotSDN, Hong Kong, 2013, pp. 165–166.

[12] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications and issues," in Proc. Mobidata, Hangzhou, 2015, pp. 37–42.

[13] 3GPP, "TR 28.801: Study on Management and Orchestration of Network Slicing," Release 17, 2022.

[14] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," BMJ, vol. 372, p. n71, 2021.

[15] MITRE, "ATT&CK for Mobile v13," 2023. [Online]. Available: https://attack.mitre.org/matrices/mobile/

[16] H. Zhang, N. Liu, X. Chu, K. Long, A. H. Aghvami, and V. C. M. Leung, "Network slicing based 5G and future mobile networks," IEEE Commun. Mag., vol. 55, no. 8, pp. 138–145, 2019.

[17] X. Li, M. Samaka, H. A. Chan, D. Bhamare, L. Gupta, C. Guo, and R. Jain, "Network slicing for 5G: Challenges and opportunities," IEEE Internet Comput., vol. 21, no. 5, pp. 20–27, 2021.

[18] Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran, "Security in software-defined networking: Threats and countermeasures," Mobile Netw. Appl., vol. 21, no. 5, pp. 764–776, 2020.

[19] A. Dalgkitsis, M. Louta, and G. Karetsos, "SCHE-IDS: GNN-based intrusion detection for cross-slice attack detection in 5G," IEEE Trans. Mobile Comput., vol. 21, no. 11, pp. 4010–4022, 2022.

[20] S. A. Mehdi, J. Khalid, and S. A. Khayam, "SHIELD-5G: Byzantine fault-tolerant distributed SDN control for 5G mobile backhaul security," IEEE Trans. Inf. Forensics Secur., vol. 17, pp. 2841–2856, 2022.

[21] M. Pattaranantakul, R. He, Q. Song, Z. Zhang, and A. Meddahi, "NFV security survey: From use case driven threat analysis to state-of-the-art countermeasures," IEEE Commun. Surveys Tuts., vol. 22, no. 1, pp. 408–436, 2020.

[22] A. Papagiannakis, G. Xilouris, C. Tranoris, A. Kourtis, and S. Spirou, "SecMANO: Secure management and orchestration for NFV environments," Comput. Netw., vol. 225, p. 109659, 2023.

[23] T. T. Nguyen, G. Armitage, P. Branch, and S. Zander, "A survey of techniques for internet traffic classification using deep learning," IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2781–2803, 2021.

[24] P. Papadopoulos, P. Agrawal, G. Iosifidis, L. Tassiulas, and T. Bourchas, "Machine learning for 5G security: A survey," IEEE Access, vol. 10, pp. 112248–112275, 2022.

[25] A. Thantharate, R. Parekh, P. Ullagaddi, P. Thantharate, and C. Beard, "DeepSlice: A deep learning approach towards an efficient and reliable network slicing in 5G networks," in Proc. IEEE IEMCON, Vancouver, 2019, pp. 762–767.

[26] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. Aguera y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proc. AISTATS, Fort Lauderdale, 2017, pp. 1273–1282.

[27] S. I. Popoola, B. Adebisi, M. Hammoudeh, G. Gui, and H. Gacanin, "Federated deep learning for zero-day botnet attack detection in IoT-edge devices," IEEE Internet Things J., vol. 9, no. 5, pp. 3930–3944, 2021.

[28] M. A. Rahman, F. Mansoor, A. S. Almadhor, T. Ahmed, and F. Al-Turjman, "Federated learning for Open RAN security: A distributed xApp intrusion detection framework," Future Gener. Comput. Syst., vol. 148, pp. 582–596, 2023.

[29] Y. Wang, J. Yang, X. Liu, and J. Yu, "DQN-based moving target defence for SDN-enabled 5G networks," IEEE Trans. Veh. Technol., vol. 71, no. 4, pp. 4356–4369, 2022.

[30] E. A. Jorswieck, H. Karl, H. D. Schotten, and A. Wolf, "Physical layer security in 5G networks: From theory to practice," IEEE Commun. Mag., vol. 59, no. 5, pp. 56–62, 2021.

[31] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," IEEE Internet Things J., vol. 6, no. 5, pp. 8169–8181, 2020.

[32] G. Shen, J. Zhang, A. Marshall, L. Peng, and X. Wang, "Radio frequency fingerprint identification for narrowband systems, modelling and classification," IEEE Trans. Inf. Forensics Secur., vol. 16, pp. 3974–3987, 2021.

[33] A. Al-Shawabka, F. Restuccia, S. D'Oro, T. Jian, X. Costa-Perez, T. Melodia, and T. Imbiriba, "Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting," in Proc. IEEE INFOCOM, Vancouver, 2021, pp. 1–10.

[34] R. Bonetto, C. Campolo, A. Iera, and A. Molinaro, "Security analysis of the O-RAN E2 interface through protocol fuzzing," IEEE Trans. Netw. Serv. Manag., vol. 20, no. 3, pp. 3187–3201, 2023.

[35] GSMA, "Open RAN Operator Deployment Tracker Q1 2024," GSM Association, London, 2024.

[36] J. H. Park, J. Moon, and M. Kim, "TEE-RAN: Trusted execution environment-based security for open radio access networks," IEEE Wireless Commun. Lett., vol. 11, no. 8, pp. 1724–1728, 2022.

[37] US Executive Office of the President, "Executive Order 14028: Improving the Nation's

Cybersecurity," Fed. Register, vol. 86, no. 93, pp. 26633–26653, 2021.

[38] R. Abdallah, N. Wang, and G. Bhaskara, "SBOM-based supply chain security for Open RAN xApp deployments," in Proc. IEEE ICC, Rome, 2023, pp. 1–7.

[39] NIST, "Cybersecurity Framework (CSF) 2.0," National Institute of Standards and Technology, Gaithersburg, MD, 2024.

[40] NIST, "Post-Quantum Cryptography Standards: FIPS 203/204/205," National Institute of Standards and Technology, 2024.

[41] ITU-R, "IMT-2030 (6G) Framework Recommendation," International Telecommunication Union, Geneva, 2023.

[42] S. Gera, S. Nehra, and J. Kathuria, “The evolving cybersecurity paradigm: New threats old vulnerabilities, strategic solutions in the information age,” International Journal of Research Publication and Reviews, vol. 6, Special Issue 5, pp. 430–451, May 2025. doi: 10.55248/gengpi.6. sp525.1960.