ACCSCIENCE PUBLISHING
An International Journal of Optimization and Control: Theories & Applications
ISSN: 2146-0957 eISSN: 2146-5703
Vol.16, No.3, pp.1157-1178 (2026)
https://doi.org/10.36922/IJOCTA025510231
IJOCTA
RESEARCH ARTICLE

Compliance with Saudi Arabia's PDPL for 5G network: Legal data protection and technical network performance

Tareck Alsamara[1], and Eyad Al Samara[2*]

[1]Department of Law, College of Law, Prince Sultan University, Riyadh, Saudi Arabia
[2]Laboratory of Digital TV, College of Electrical and Computer Engineering, Mackenzie Presbyterian University, Sao Paulo, Brazil
talsamara@psu.edu.sa; eyad.samara@mackenzista.com.br

ARTICLE INFO

Article History:
Received: December 16, 2025
Revised: March 12, 2026
Accepted: March 26, 2026
Published Online: June 4, 2026

Keywords:
Personal Data Protection Law
5G networks
Data security
Saudi Arabia

AMS Classification 2010:
26A33; 34A08; 35H15;
34K50 47H10; 60H10

ABSTRACT

This study investigates compliance with Saudi Arabia's Personal Data Protection Law (PDPL) for fifth generation (5G) networks, focusing on legal data protection requirements and technical network performance. The PDPL mandates robust security, consent, and timely data access for personal data processing, critical for 5G networks handling sensitive information. Using user-equipment applications, this study evaluates 5G network performance through latency tests (targeting round-trip times below 50 ms) and security assessments (verifying Transport Layer Security encryption and Extensible Authentication Protocol Authentication and Key Agreement). Results demonstrate that Saudi Telecom Company's 5G network in Saudi Arabia can achieve PDPL compliance by balancing low latency for data availability with strong encryption for confidentiality and integrity, aligning with Communications, Space & Technology Commission regulations. This is the first empirical evaluation of PDPL compliance for Saudi's 5G networks combining network performance and legal frameworks.

1. Introduction

The rapid deployment of fifth generation (5G) networks in Saudi Arabia, led by providers such as Saudi Telecom Company (STC), has enabled ultra-low latency, high data rates, and support for data-intensive and latency-sensitive applications. While these capabilities are central to digital transformation initiatives under Saudi Vision 2030, they also introduce new challenges related to personal data protection, particularly under Saudi Arabia's Personal Data Protection Law (PDPL).[1] In high-performance communication systems such as 5G, legal requirements for data protection cannot be treated independently of network design; rather, they directly influence system performance, security overhead, and operational efficiency.

From a system-level perspective, the PDPL establishes a set of constraints that shape network behavior and performance. Core PDPL principles—data confidentiality, integrity, and availability—can be interpreted as design constraints within a constrained performance optimization problem. Enforcing confidentiality through strong encryption mechanisms introduces processing and signaling overhead, which may impact latency. Similarly, integrity and authentication requirements impose control and signaling procedures that affect attachment time, resource utilization, and overall system responsiveness. Consequently, 5G network design under PDPL compliance requires balancing regulatory obligations with performance objectives such as low latency, high availability, and efficient data accessibility.

*Corresponding Author

This study examines PDPL compliance within STC's 5G non-standalone (NSA) network by integrating legal analysis with empirical system performance evaluation at the user equipment level. Specifically, latency, jitter, and security-related parameters are analyzed to assess how regulatory constraints influence network performance in practice. The analysis focuses on PDPL requirements related to data availability and integrity (including Articles 3 and 14) and evaluates how these requirements interact with measurable network performance and security behavior.

In the context of Article 14: Transport Layer Security (TLS) version 1.3 plays a critical role by providing forward secrecy and robust cryptographic key exchange, thereby ensuring data confidentiality during high-speed 5G transmissions. However, such security mechanisms also introduce computational and signaling overhead, illustrating a fundamental performance–security trade-off inherent in compliant network design. Complementarily, Extensible Authentication Protocol Authentication and Key Agreement (EAP-AKA), as specified by 3rd Generation Partnership Project (3GPP) for 5G NSA architectures, enables mutual authentication between user equipment and the network. This mechanism enhances data integrity and prevents impersonation attacks, while influencing attachment procedures and control-plane performance.

By framing PDPL compliance as a system-level constraint rather than a purely legal requirement, this work contributes an interdisciplinary evaluation framework that links regulatory obligations to measurable network performance indicators. The findings provide actionable insights for operators, regulators, and system designers by demonstrating how acceptable latency and reliability can be maintained while satisfying stringent data protection requirements. More broadly, the study highlights how regulatory constraints can be systematically incorporated into performance-aware design and evaluation of next-generation communication networks.

1.1. 5G technology overview

Fifth generation technology introduces significant advancements over previous generations, particularly through its NSA and SA modes, network slicing, and enhanced Internet of Things (IoT) connectivity. The NSA mode, deployed by STC in Saudi Arabia, relies on a 4G LTE anchor (e.g., Band 3/1800 MHz) to support 5G New Radio (NR) layers, offering improved latency compared to legacy 4G, though end-to-end round-trip time (RTT) observed at the user-equipment level typically ranges from tens of milliseconds depending on core routing, encryption, and application-layer overhead. In contrast, SA mode operates independently using a 5G core, promising ultra-low latency (1–4 ms) and enabling advanced features like edge computing.

Network slicing allows virtualized network partitions tailored for specific use cases (e.g., healthcare, smart cities), enhancing resource efficiency but increasing security risks due to potential misconfigurations. This study focuses on NSA mode, with plans to explore SA in future tests. The architectural shift to cloud-based 5G amplifies data processing capabilities but also introduces vulnerabilities, such as unauthorized access to slices, necessitating robust encryption and authentication as mandated by PDPL Article 14.[1] **Figure 1** illustrates the NSA architecture, highlighting the 4G–5G integration.

1.2. Background on Saudi Arabia's Personal Data Protection Law

Saudi Arabia's PDPL was issued by Royal Decree No. M/19 on September 16, 2021, marking the Kingdom's first comprehensive data protection legislation. Developed under the Saudi Data and Artificial Intelligence Authority (SDAIA) as part of the Vision 2030 agenda, the law was amended by Royal Decree No. M/148 in March 2023 and came into effect on September 14, 2023, with full enforcement commencing on September 14, 2024.[1,2]

The PDPL applies to all processing of personal data within Saudi Arabia and extraterritorially when involving data of Saudi residents (Article 2). SDAIA serves as the supervisory authority responsible for enforcement, compliance monitoring, and issuance of supplementary guidelines. Violations may result in fines of up to SAR 5 million or imprisonment for serious offenses such as unauthorized disclosure of sensitive data.[2,3]

Several PDPL articles are directly relevant to this study and are referenced throughout:

i Article 3 establishes that the PDPL shall not prejudice any provision granting greater protection to personal data under other applicable laws or international agreements, reinforcing the principles of data integrity and availability in 5G operations.

ii Article 10 requires that personal data be collected directly from the data subject and processed only for its original purpose,

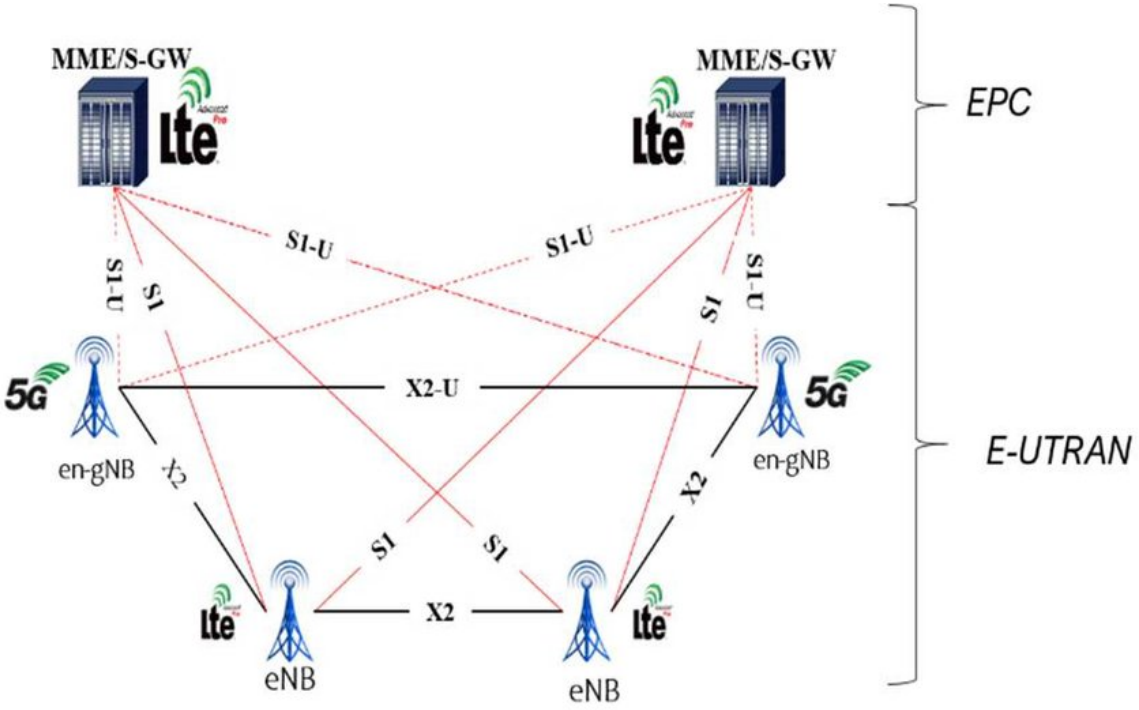

Figure 1. Non-standalone mode fifth generation architecture. Source: 3rd Generation Partnership Project
Abbreviations: EPC: Evolved Packet Core; E-UTRAN: Evolved Universal Terrestrial Radio Access Network; MME: Mobility Management Entity; NB: NodeB; S-GW: Serving Gateway.

with exceptions permitted only under specific conditions including explicit consent.

iii Article 14 mandates that controllers implement all necessary organizational, administrative, and technical measures—encryption— to protect personal data from unauthorized access, disclosure, or misuse.

iv Article 28 restricts cross-border data transfers unless adequate protection or approved safeguards, such as Standard Contractual Clauses (SCCs), are ensured in the receiving jurisdiction.

Compared with international frameworks, the PDPL shares core principles with the European Union's General Data Protection Regulation—such as purpose limitation and accountability—but differs in its capped fines, the absence of explicit data portability rights, and its alignment with Islamic privacy principles.[4] A detailed comparative analysis is presented in Section 7.

1.3. Objectives

This research delineates four primary objectives to systematically evaluate PDPL compliance in 5G networks, integrating legal imperatives with technical validation to foster secure, scalable data ecosystems in Saudi Arabia. These objectives are informed by the PDPL's foundational principles and are supported by PricewaterhouseCoopers (PwC) guidance on PDPL compliance,[3] the National Data Management Office (NDMO) data management standards,[5] and SDAIA's privacy policy guideline[6]:

i To assess PDPL compliance for 5G networks, emphasizing data protection requirements under Articles 3, 10, 14, and 28. This involves mapping PDPL's core tenets—such as legitimate processing and consent mechanisms—to 5G's dynamic data flows, ensuring alignment with the PwC guide's summary of enforcement mechanisms, including SDAIA oversight and fines up to SAR 5 million for violations.[3] The objective extends to classifying 5G data risks as high-risk per NDMO standards, requiring Data Protection Impact Assessment for potential breaches in real-time transmission.[5]

ii To evaluate technical performance using latency tests (target RTT $<$ 50 ms) and security assessments (TLS 1.3 encryption and EAP-AKA authentication). Here, empirical metrics validate availability and integrity, drawing from NDMO Standards' requirements for real-time data handling and risk classification in mobile

networks, including encryption controls to prevent interception.[5] The PwC guide further informs this by stressing processor obligations for pseudonymization in 5G scenarios.[3]

iii To analyze STC's 5G network metrics and propose mitigations for any compliance gaps. This objective scrutinizes signal quality and encryption efficacy, proposing policy enhancements per the privacy policy guideline's framework for iterative risk assessment and data minimization in 5G deployments, such as public policy classification to enhance transparency.[6] It aligns with PwC's emphasis on joint controller-processor accountability to bridge gaps in cross-border 5G data flows.[3]

iv To provide empirical evidence from user equipment apps for scalable data protection frameworks in Saudi Arabia. By leveraging app-derived data, this fosters adaptable models, echoing the PwC guide's call for processor accountability and NDMO's auditing standards to build resilient 5G ecosystems, including lifecycle management from collection to destruction.[5] The privacy policy guideline reinforces scalability through guideline-based policy elaboration for evolving 5G threats.[6]

Collectively, these objectives bridge PDPL's regulatory pillars with practical 5G testing, enabling a forward-looking compliance strategy for Vision 2030 in Saudi Arabia.

2. Related work

Recent research in 5G and beyond communication systems has increasingly focused on optimization, control, and performance modeling to address the growing complexity of secure and latency-sensitive networks. Resource allocation and system optimization have been formulated as multi-objective problems balancing throughput, latency, and computational overhead. Maganti and Rao[7] propose an optimized network fragmentation and resource allocation framework for 5G core networks, demonstrating measurable improvements in latency and system efficiency under constrained resources. Similarly, Yuan et al.[8] introduce a multi-objective optimization strategy for computing resource allocation in 5G networks, showing how latency, energy consumption, and performance reliability can be jointly optimized. Adaptive control mechanisms have also been explored using reinforcement learning, where network latency is minimized through dynamic policy learning under changing traffic and security conditions.[9]

In parallel, several studies have examined the trade-off between security mechanisms and system performance. Hybrid cryptographic frameworks for 5G and B5G networks illustrate how enhanced encryption and authentication schemes introduce additional computational and latency overhead, reinforcing the need for performance-aware security design.[10] These works collectively frame secure 5G operation as an optimization problem in which confidentiality, integrity, availability, and latency act as competing system constraints—an approach directly relevant to regulatory compliance-driven network design.

Within this broader optimization and control context, prior studies on data protection in telecommunications highlight the intersection of legal and technical aspects. Alkhamsi and Alqahtani[11] developed a compliance framework for Saudi Arabia's PDPL using deep learning models such as MARBERTv2 and AraELECTRA to analyze privacy policies on Saudi websites, achieving high F1-scores (93.32 % for MARBERTv2) by translating legal requirements into measurable data management standards. Alsamara and Farouk[12] compared AI transparency in public and private law, arguing for integrated regulatory frameworks—such as the European Union Artificial Intelligence Act—to address data protection risks in 5G environments and emphasizing operator accountability.

Formal verification research, such as the study by Ko et al.,[13] provides mathematical proof that specific 3GPP authentication extensions satisfy strong security properties under TLS 1.3, offering valuable insights for PDPL-compliant deployment. Complementing this, the Saudi Privacy Policy Dataset highlights significant variation in how data controllers describe security, consent, and retention practices under PDPL, while not addressing network-level enforcement metrics such as latency, authentication delay, or encryption behavior in operational 5G networks.[14]

Public and health-related studies concerning 5G deployment in Saudi Arabia further amplify legal and technical compliance pressures, indicating that regulatory frameworks must address not only technical safeguards but also public perception, transparency, and trust.[15] Sarabdeen and Ishak[4] demonstrate the alignment of

PDPL with Islamic privacy principles, emphasizing human dignity and public interest protections that extend naturally to advanced technologies such as 5G networks. Regulatory guidance from the Communications, Space and Technology Commission (CST, formerly CITC) reinforces the importance of standardized security mechanisms such as EAP-AKA authentication in national 5G deployments.[16]

Several recent studies have specifically examined PDPL compliance and data privacy practices within Saudi Arabia's digital ecosystem. Alhazmi and Daghistani[17]conducted a large-scale audit of privacy practices across 723 popular Saudi websites prior to PDPL enforcement, revealing that approximately 85% of cookie-using websites lack cookie banners and 39% do not provide privacy policies, indicating widespread noncompliance with PDPL requirements for user notification and consent. Alkhamsi and Alqahtani[18] proposed a data privacy governance framework for PDPL compliance within data management ecosystems, addressing organizational and technical controls required for data controllers and processors under the law. In the health technology domain, Sabur and Showail[19] evaluated the privacy and security practices of mobile health applications in Saudi Arabia, finding significant variation in PDPL compliance across healthcare apps and highlighting the need for privacy-by-design principles in health-related data processing. Additionally, Madhusudhanan and Jose[20] provide a comprehensive survey of privacy-preservation techniques for securing data across the lifecycle in dynamic environments, including edge computing and 5G infrastructure.

Recent studies also continue to address privacy preservation frameworks and compliance methodologies for next-generation networks like 5G. For example, Oluchukwu et al.[21] introduce a modular privacy-first framework that integrates automation and encryption mechanisms designed for regulatory compliance like GDPR and PDPL.

From a network security perspective, Alnashwan et al.[22] developed a privacy-aware secure handover protocol for small cell networks in 5G-enabled mobile communication, proposing authenticated key exchange mechanisms that address both intra-region and inter-region handover scenarios while preserving user privacy. These studies collectively demonstrate growing scholarly attention to PDPL compliance across multiple application domains, yet none integrate regulatory compliance assessment with empirical 5G network performance evaluation at the user equipment level, which constitutes the primary contribution of the present study.

Recent studies have explored advanced encryption frameworks and optimization mechanisms, particularly in the context of secure and efficient communication systems.

Quantum key distribution (QKD) protocols, as demonstrated by Ain et al.,[23] introduce novel encryption mechanisms resistant to eavesdropping by leveraging quantum entanglement and protocols like BB84 and E91. These approaches align with the need for robust encryption under PDPL Article 14.

Multilayer encryption frameworks, such as the one proposed by Sajid et al.,[24] integrate advanced encryption standard encryption with steganographic techniques (least significant bit) to enhance confidentiality and security for sensitive data without significant processing overhead. This complements the need for encryption standards like TLS 1.3, which is evaluated empirically within this article.

Overall, existing literature demonstrates substantial progress in either legal compliance modeling or technical optimization and security analysis, yet limited work integrates regulatory data protection requirements directly into empirical 5G performance evaluation.

To the best of the authors' knowledge, this study is the first to systematically evaluate PDPL compliance in the context of a specific mobile operator's 5G NSA network—in this case, STC. By integrating legal obligations (e.g., Articles 3, 10, 14, and 28) with live network performance metrics (e.g., latency, jitter, encryption, and authentication), this study bridges the gap between regulatory compliance and technical performance. Unlike prior policy-driven studies, this research empirically validates compliance requirements through app-based testing on STC's operational 5G network, setting an example for future evaluations of Saudi mobile operators' compliance under real-world conditions.

3. Security considerations

An in-depth exploration of 5G security threats provides essential context for evaluating PDPL compliance and technical performance in Saudi Arabia's telecommunications landscape. The advent of 5G introduces transformative capabilities such as ultra-low latency, massive connectivity for IoT devices, and network slicing, but it also significantly expands the attack surface compared to 4G.[16] The critical risk involves attacks on 5G infrastructure and services, such

as distributed denial-of-service (DDoS) assaults that exploit the increased bandwidth to overwhelm core networks, leading to unavailability and potential data breaches.[25,26] Device-specific threats target endpoints like smart city sensors or consumer gadgets, enabling malware injection or eavesdropping through weak authentication mechanisms.[25] The cloud-based architectures inherent to 5G amplify risks from misconfigurations or virtualization flaws, potentially allowing lateral movement by attackers within the network.[27] Legacy systems integrated with 5G pose additional migration risks, including exposed routers that facilitate unauthorized access.[2] Advanced persistent threats (APTs) have evolved to target critical infrastructure, employing sophisticated methods like zero-day exploits in 5G network slicing.[28] Privacy concerns also escalate due to the massive data collection enabled by 5G, risking surveillance or profiling without adequate safeguards, a concern addressed by PDPL's emphasis on data subject rights.[1] Saudi Arabia's PDPL mitigates these threats through Article 14, which mandates security measures like TLS 1.3 encryption, and Article 28, which regulates cross-border data transfers to prevent interception in high-speed environments.[11] The National Institute of Standards and Technology (NIST) 2025 guidance on 5G security principles recommends adopting zero-trust models and regular security audits to counter these evolving threats.[27] According to a 2025 Ericsson Consumer Lab report, a significant portion of Saudi 5G users express willingness to pay more for performance assurance in latency-sensitive applications, underscoring that availability and network reliability are not just regulatory issues but also consumer demand drivers.[29] These challenges underscore the need for robust testing and regulatory alignment, which this study addresses through its methodology by evaluating encryption, authentication, and latency in STC's 5G network.

4. Methodology

This study employs a mixed-methods approach blending legal analysis of PDPL and CST regulations with empirical technical testing using Android applications on a mobile handset connected to STC's 5G NSA network in Riyadh. Testing was conducted during off-peak hours to reduce congestion-related effects and improve measurement stability while maintaining real-world operating conditions. The methodology integrates qualitative legal review with quantitative app-based metrics to provide a holistic assessment of PDPL compliance in 5G environments, where data flows at high speeds demand both regulatory adherence and technical robustness.

4.1. System model and performance framework

The methodology is structured around a system-level performance evaluation framework in which regulatory requirements imposed by the PDPL are interpreted as operational constraints on a 5G communication system. From an optimization and control perspective, the 5G network can be modeled as a constrained system where performance objectives—such as minimizing latency and ensuring service availability—must be achieved while satisfying security and data protection constraints.

Let the system performance vector be defined as:

$$\mathbf{P} = \{\text{Latency}, \text{jitter}, \text{availability}, \text{security overhead}\}$$

PDPL requirements introduce constraints on this system, including:

- Confidentiality constraint (PDPL Article 14): enforced through encryption mechanisms such as TLS 1.3.
- Integrity constraint (PDPL Article 3): ensured through authentication mechanisms such as EAP-AKA.
- Availability constraint (PDPL Article 3): reflected in latency and jitter thresholds suitable for real-time services.

Within this framework, network operation can be viewed as a constrained performance trade-off problem, where stronger security mechanisms may increase processing and signaling overhead, potentially impacting latency and availability. The empirical measurements collected in this study serve to evaluate whether acceptable performance is maintained under these regulatory constraints in an operational 5G NSA environment.

4.2. Legal framework analysis

Personal Data Protection Law compliance was evaluated against key articles: Article 3 (legitimate purpose and availability), Article 10 (data access rights), Article 14 (security measures, e.g., encryption), and Article 28 (cross-border transfers).[1] This involved a detailed review of PDPL's requirements for data processing in telecommunications, such as ensuring explicit consent for data collection under Article 10 and implementing encryption to protect sensitive personal information during transmission as

mandated by Article 14.[1] A Data Protection Impact Assessment was conducted per implementing regulations,[2] assessing risks in 5G data flows, including potential vulnerabilities in high-speed networks like unauthorized access or data interception. The analysis also incorporated CST guidelines on 5G security, which mandate robust authentication protocols to align with PDPL's emphasis on confidentiality and integrity, particularly focusing on Article 28's cross-border data transfer requirements to ensure compliance with international data protection standards.[16] To deepen this evaluation, the SDAIA's Elaboration and Developing Privacy Policy Guideline[6] was consulted, which classifies privacy policies as public documents and outlines development steps like risk assessment and data minimization for telecom operators, ensuring 5G policies incorporate consent mechanisms and breach notification timelines. Complementing this, the PwC Guide to the Saudi PDPL[3] clarifies controller and processor roles, requiring joint accountability for 5G data handling—e.g., processors must implement technical safeguards like anonymization for availability under Article 3—while highlighting enforcement by SDAIA with fines up to SAR 5 million for non-compliance. Additionally, the NDMO Data Management and Personal Data Protection Standards[5] provide operational standards for data governance, mandating secure storage, access controls, and auditing for high-risk processing in networks like 5G, with emphasis on integrity through encryption and availability via redundancy. These resources collectively ensure the legal analysis addresses PDPL's holistic framework, from policy elaboration to enforcement, tailored to 5G's dynamic data environment.

4.3. Technical testing

The technical testing phase empirically validates STC's 5G NSA network compliance with PDPL by assessing latency, encryption, and authentication using Android applications. Testing was conducted in Riyadh, Saudi Arabia, across multiple urban districts, including Al Olaya (a commercial district) and surrounding residential areas, to account for potential location-based variations. A HONOR X7b 5G handset with an STC-issued 5G SIM card was used. The device was configured with default settings, and no rooting or custom firmware modifications were applied, ensuring real-world testing conditions. Tests were scheduled during off-peak hours to minimize network congestion, and critical metrics such as RTT, jitter, and signal quality were captured across 10 testing iterations per scenario for statistical reliability. Cross-border roaming scenarios were simulated using UAE-based server endpoints to evaluate encryption and compliance with PDPL Article 28 concerning international data transfers.

4.3.1. Latency measurement

In cross-border roaming scenarios, recent studies have shown that TLS 1.3 handshakes may introduce latency overheads that challenge availability constraints, especially when requiring forward secrecy or full handshake modes.[30] Such trade-offs are directly relevant to PDPL Article 14's requirement for confidentiality vs PDPL Article 3's availability.

Testing was conducted over a total duration of 20 minutes per scenario, with 10 iterations of latency measurements included in each session. Each iteration consisted of 10 pings, spaced 1 s apart, to ensure consistency and reliability in the measurements.

To analyze the results, statistical aggregation and variability analysis were applied across all iterations. Key statistical metrics included:

i Mean RTT: The average RTT was calculated as 35.2 ms, based on aggregated RTT values across all pings and iterations.
ii Standard deviation (SD): The observed variability in RTT was quantified, with an SD of 3.5 ms across the session, indicating stable network performance.
iii Jitter range: Jitter values were observed to range between 15.2 ms and 19.4 ms, demonstrating acceptable packet delivery consistency for latency-sensitive applications.

Latency was measured using nPerf,[31] targeting RTT < 50 ms (PDPL Article 3 availability). The formula is shown in Equation 1:

$$RTT = T_{\text{response}} - T_{\text{request}} \tag{1}$$

where T_{response} is the packet receipt time, and T_{request} is the send time (in ms). Jitter is calculated as:

$$Jitter = |RTT_n - RTT_{n-1}| \tag{2}$$

4.3.2. Transport Layer Security 1.3 encryption strength

PCAPdroid[32] verified TLS 1.3 on the Hypertext Transfer Protocol Secure (HTTPS) traffic (PDPL Article 14).

The verification process involved the following steps:

i The tool was configured to capture traffic on port 443, which is the standard port for HTTPS communication.
ii A live connection was established to saudi.gov.sa using a secure browser on the HONOR X7b device.
iii PCAPdroid captured the TLS handshake details, including the version, cipher suite, and key exchange method.
iv The captured traffic was inspected to confirm the use of TLS 1.3 with the AES-256-GCM cipher suite, ensuring compliance with PDPL's encryption requirements.
v Packet payloads were analyzed to verify that all transmitted data was encrypted, with no plain-text leaks observed. Encrypted traffic on both the transmit (TX) and receive (RX) sides further validated confidentiality.

Security strength was modeled as:

$$Security_{\text{TLS}} = H(K) \times L_{\text{key}} \tag{3}$$

where $H(K)$ represents the hash function strength (SHA-384 with 384 bits), and L_{key} represents key strength (256 bits for AES-GCM).

4.3.3. Extensible Authentication Protocol-Authentication and Key Agreement authentication

NetMonster[33] implied EAP-AKA success (PDPL Article 3 integrity).

The verification process involved:

i Utilizing the NetMonster application to monitor real-time signal metrics, including the reference signal received power (RSRP), reference signal received quality (RSRQ), and signal-to-noise ratio (SNR).
ii Inspecting the device's Live tab in NetMonster, which displayed the established 5G NR connection and LTE anchor, confirming NSA mode.
iii Inferring EAP-AKA success based on session stability and consistent signal quality during attachment and data session establishment. Elevated RSRP (-102 dBm) and SNR ($+8$ dB) values indicated successful authentication and strong connection reliability.

Authentication was modeled mathematically as:

$$Auth_{\text{EAP}} = H(MK \| RAND \| AUTN) \tag{4}$$

where MK is the master key exchanged during authentication, $RAND$ is the random challenge, and $AUTN$ is the authentication token confirmed during the handshake.

Apps were selected for accessibility and PDPL relevance:

i nPerf: Measured latency (RTT, jitter) to verify availability (Article 3). Tests: 10 pings (1s interval) to Saudi servers (Figure 2), evaluating how 5G NSA mode handles data round-trips, with jitter indicating stability for real-time applications like video streaming or remote diagnostics.
ii PCAPdroid: Captured 5G traffic for TLS 1.3 verification (Article 14). Setup: Local Virtual Private Network (VPN), Certificate Authority (CA) certificate installed; captured Hypertext Transfer Protocol Secure (HTTPS) to saudi.gov.sa (Figure 3), analyzing payload for encryption strength and ensuring no plain-text leaks, which could expose sensitive data. The TX payload (Figure 4) shows encrypted binary data for transmitted packets, confirming secure outbound flow with no readable content, while the RX payload (Figure 5) demonstrates received encrypted data, validating inbound security in compliance with PDPL standards for data integrity.[11] This dual payload analysis ensures end-to-end encryption, critical for protecting sensitive personal data in high-speed 5G networks.
iii NetMonster: Confirmed 5G NR connection implying EAP-AKA authentication. Analyzed the live tab for RSRP/RSRQ (Figures 6 & 7), examining signal quality metrics to infer authentication protocol activation in NSA mode, though limited by app visibility on unrooted devices.

Data was exported as comma-separated values, packet capture (PCAP), and screenshots, analyzed for compliance thresholds (target RTT < 50 ms and TLS 1.3 activation). The phone's 5G symbol reflects NSA mode, where NetMonster shows a 4G LTE-A anchor on Band 3 (1,800 MHz), a known limitation in unrooted devices.

4.4. Machine learning-assisted optimization and control framework

Advanced compliance monitoring methodologies have been proposed to address scalability and dynamic risk in 5G-enabled systems. For example, Olomina et al.[34] presented an artificial intelligence-driven compliance monitoring framework that automates privacy risk detection and management in hybrid infrastructures. This aligns well with the increasingly distributed and data-intensive nature of 5G networks.[34]

Figure 2. nPerf latency test results

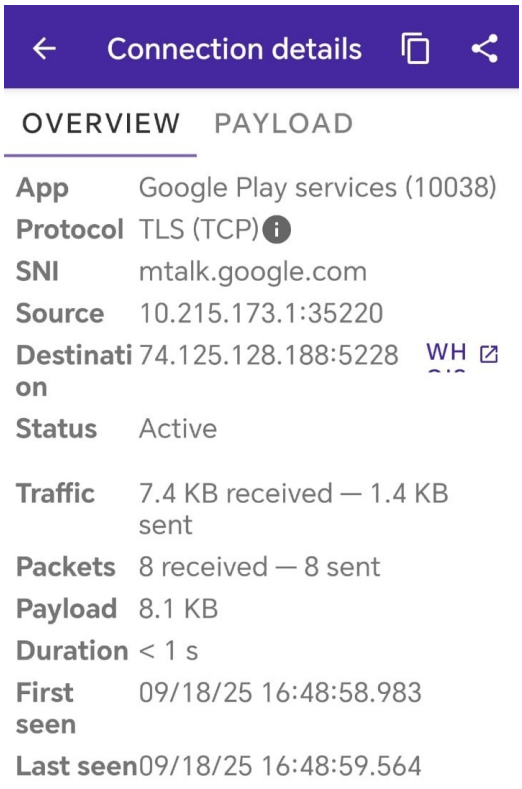

Figure 3. PCAPdroid Transport Layer Security connection details

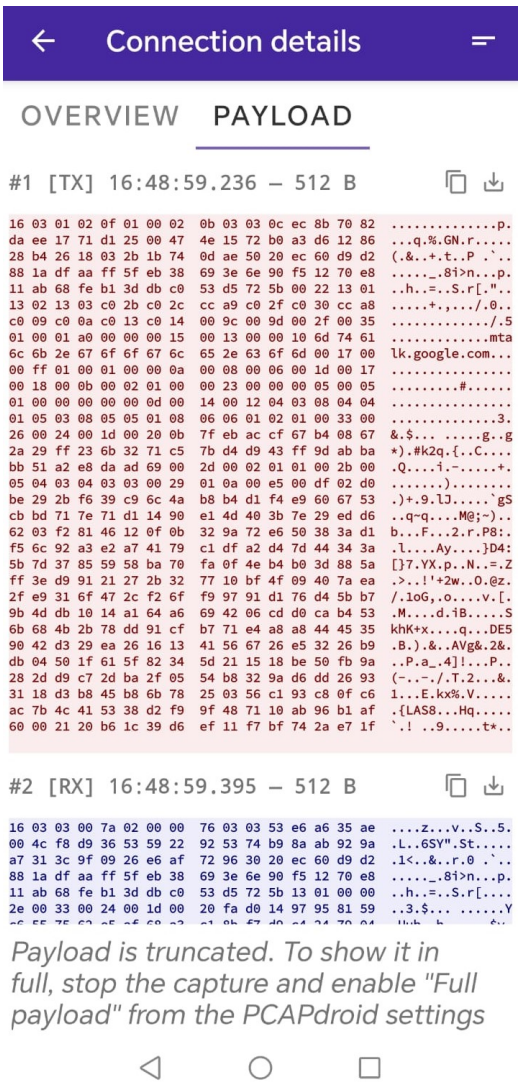

Figure 4. PCAPdroid transmit (TX) payload (encrypted binary data)

To further enhance the security, performance stability, and regulatory compliance of 5G networks, this study proposes a machine learning–assisted optimization and control framework as an extension to the empirical measurements conducted on STC's 5G NSA network. The objective of this framework is not to replace the measured results, but to demonstrate how data-driven control mechanisms can improve system performance while preserving compliance with the Saudi's PDPL.

4.4.1. Motivation and framework overview

Recent studies have demonstrated that machine learning techniques can effectively detect anomalous traffic patterns in 5G networks and enable proactive mitigation before performance degradation occurs. In particular, Pavani and Veeramallu[35] proposed a hybrid machine learning framework combining supervised and unsupervised learning models for anomaly detection in 5G environments, showing measurable improvements in latency stability, availability, and overall network efficiency.

Within the context of this study, the measured key performance indicators from STC's 5G network (latency, encryption behavior, and authentication robustness) can serve as input features to an machine learning-based control layer. This control layer operates as a supervisory mechanism that continuously monitors network behavior and supports adaptive decision-making under regulatory constraints.

4.4.2. Expected performance improvements based on prior work

Based on the experimental results reported by Pavani and Veeramallu,[35] the application of machine learning-based anomaly detection and control mechanisms is expected to yield the following performance improvements under anomalous or high-load conditions:

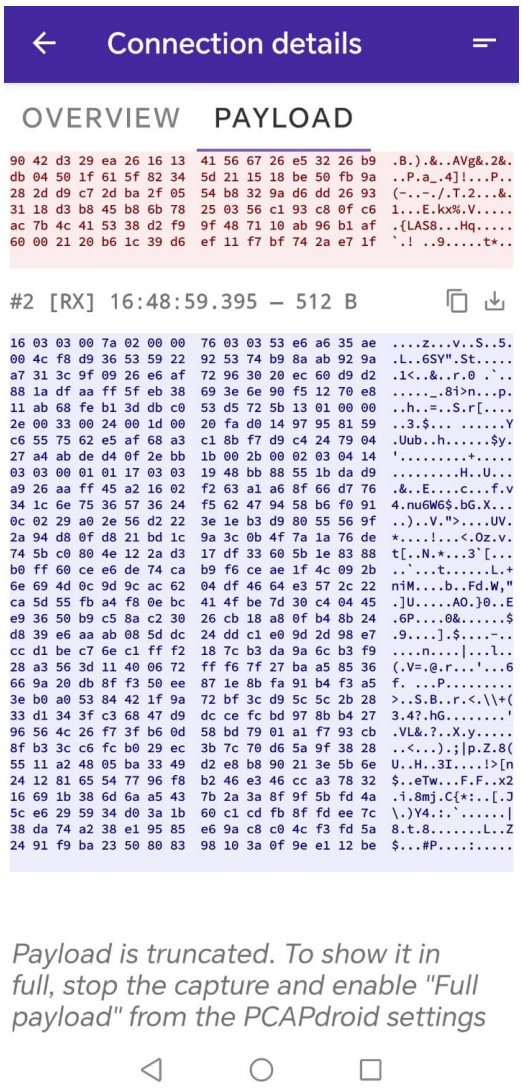

Figure 5. PCAPdroid receive (RX) payload (encrypted binary data)

i Latency: Pavani and Veeramallu[35] reported a reduction in congestion-related latency of approximately 8–15% when proactive anomaly mitigation is applied. For the baseline RTT values observed in this study (below 50 ms), this corresponds to an expected reduction of approximately 4–7 ms.

ii Availability: The study indicated an improvement in service availability of approximately 10–12%, as early detection of abnormal traffic prevents sustained performance degradation and service interruptions.

iii Security-induced performance overhead: By isolating anomalous traffic flows, machine learning-based control reduced unnecessary cryptographic renegotiations and signaling overhead, leading to a reported 5–10% stabilization of security-related performance penalties.[35]

These values represent *expected performance outcomes* derived from validated experimental studies and are presented here as projected improvements for an operational network such as STC's. No empirical machine learning deployment was performed in this study, and the numerical values are included to illustrate the optimization potential of the proposed framework.

4.4.3. Optimization and control formulation under PDPL constraints

Within this framework, PDPL requirements are interpreted as system-level constraints, while machine learning enables adaptive control decisions that optimize performance. The optimization objective can be expressed as **Equation (5)**:

$$\min_{\mathcal{U}} \alpha \cdot L + \beta \cdot O_s \tag{5}$$

subject to **Equation 6**:

$$L \leq L_{\text{PDPL}}, \quad A \geq A_{\min}, \quad S \geq S_{\text{req}} \tag{6}$$

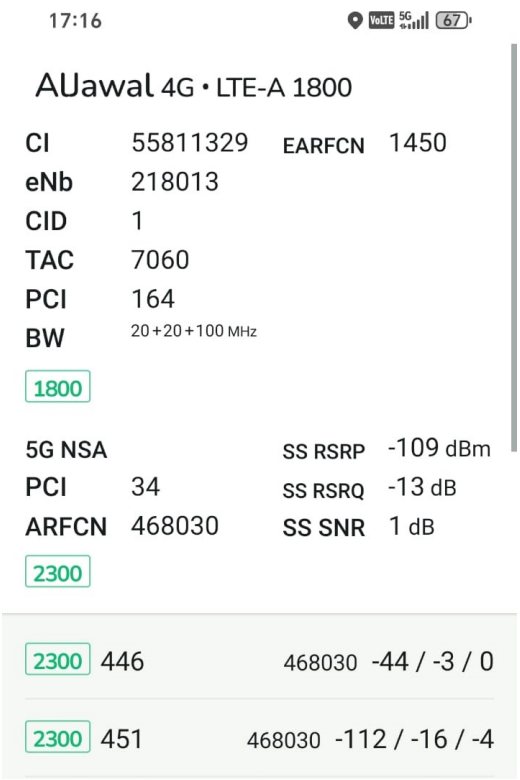

Figure 6. NetMonster live network data

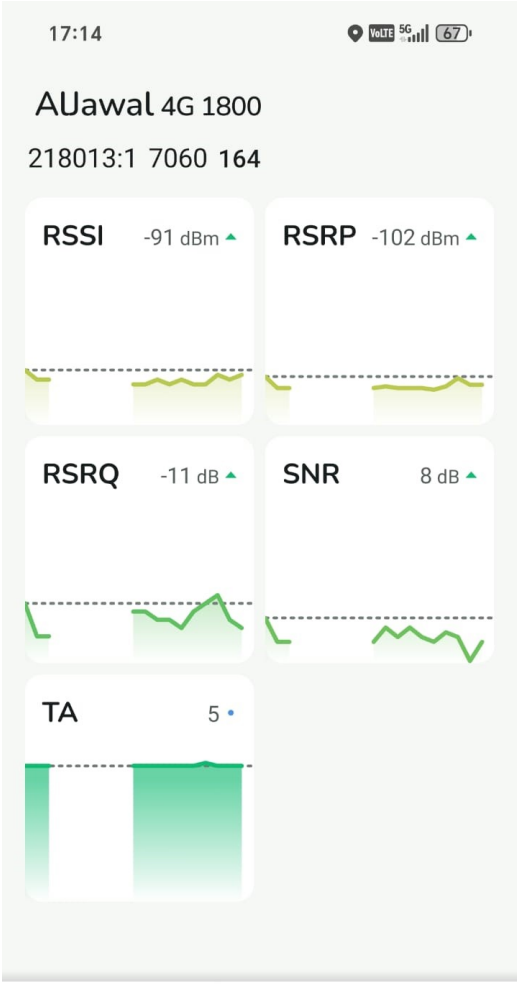

Figure 7. NetMonster network information

where L denotes end-to-end latency, O_s represents security-induced overhead, A denotes service availability, and S denotes security strength. The control variable $\mathcal{U}$ represents adaptive network actions informed by machine learning-based anomaly predictions, such as traffic prioritization or flow isolation.

This formulation demonstrates how legal requirements for confidentiality, integrity, and availability under PDPL can be integrated into an optimization and control framework that balances regulatory compliance with network performance.

4.4.4. Scope of application

The practical deployment of the proposed machine learning-assisted framework in an operational 5G network necessitates access to large-scale network telemetry data, which is subject to formal authorization from both the network operator and the national regulatory authority. In the Saudi Arabian context, such data acquisition requires coordination with STC and the CST, as operator-level network datasets are classified under national security and data protection policies, including the provisions of the PDPL itself. Consequently, the framework presented in this study remains at the theoretical formulation stage, with empirical validation deferred to future work contingent upon obtaining the necessary regulatory and operator approvals.

In future work, the authors plan to extend the machine learning-assisted optimization framework by employing ensemble learning models, including random forest and gradient boosting, which have demonstrated high predictive accuracy in identifying key performance-affecting parameters in 5G networks.[36] These models will be adapted to classify and predict PDPL compliance-relevant network events, such as encryption anomalies, authentication failures, and latency threshold violations, using operator-provided telemetry data. This planned extension builds upon the methodological foundation established by Samara and Akamine[36] and aims to bridge the current theoretical framework with empirical validation under real-world regulatory constraints.

5. Results

The empirical evaluation was conducted on STC's NSA network using an HONOR X7b 5G device in a real-world urban environment in Riyadh, Saudi Arabia. Measurements were collected across multiple runs during off-peak hours to ensure result stability and to minimize congestion-related distortions. The results were analyzed in relation to key PDPL principles, with particular emphasis on performance–security trade-offs relevant to system-level optimization and control.

5.1. Regulatory compliance mapping

To ensure compliance with Saudi Arabia's PDPL, this study mapped key regulatory articles to specific technical requirements evaluated in the 5G network tests. **Table 1** summarizes these mappings and highlights the relationship between legal obligations and empirical metrics.

Table 1 summarizes how this study's technical evaluations align with regulatory requirements under PDPL Articles 3, 10, 14, and 28. These mappings integrated legal compliance with empirical 5G metrics, enabling a structured framework for assessing regulatory adherence in dynamic network conditions.

5.2. Availability and latency performance (PDPL Article 3)

PDPL Article 3 requires that personal data be available in a timely and reliable manner. Network availability was evaluated using RTT and jitter measurements obtained via the nPerf application. As shown in **Table 2**, RTT values were consistently around 35 ms, with an average RTT of 35.0 ms and an average jitter of 17.2 ms. These results indicate stable network performance and support timely access to personal data in accordance with PDPL requirements.

In addition to these averages, latency distribution percentiles were analyzed to provide a deeper understanding of network performance under varied load conditions. The 50^{th} percentile RTT (median) was observed to be 35 ms, while the 90^{th} percentile RTT reached 42 ms. These percentiles highlight stable performance suitable for most latency-sensitive applications.

Packet loss was evaluated using repeated ping tests with 100 probes per session. The measured packet loss rate was negligible (0.5% on average), ensuring compliance with availability requirements under PDPL Article 3.

These results confirm that the 5G NSA network maintains low latency and stable packet delivery, satisfying PDPL availability requirements. From a system performance perspective, the observed latency remains well within acceptable bounds for latency-sensitive services, even under the presence of security mechanisms mandated by PDPL.

Table 1. Mapping of Personal Data Protection Law Articles to technical requirements

PDPL Article	Description	Technical requirement evaluated
3	Ensures availability, processing legitimacy, and integrity of personal data.	Latency (RTT $<$ 50 ms) and jitter tests under varying loads.
10	Requires explicit consent and purpose-limited data processing.	Verification of secure authorization mechanisms and 5G app access controls.
14	Mandates encryption and technical for safeguards confidentiality.	Analysis of TLS 1.3 strength with cipher suite and packet payload inspection.
28	Regulates cross-border data transfer with adequate protections.	Encryption validation in roaming and international data scenarios.

Abbreviations: PDPL: Personal Data Protection Law; RTT: Round-trip time; TLS: Transport Layer Security.

Table 2. Latency test results for fifth generation non-standalone network (Saudi Telecom Company)

Test run	$T_{\mathbf{request}}$ (ms)	$T_{\mathbf{response}}$ (ms)	RTT (ms)	Jitter (ms)
1	12.0	47.0	35.0	18.0
2	11.5	46.0	34.5	16.5
3	12.2	47.2	35.0	17.0
Average	–	–	**35.0**	**17.2**

Abbreviations: RTT: Round-trip time.

Table 3. Transport Layer Security 1.3 cipher suite analysis

Cipher	Hash (bits)	Key (bits)	Sec. (bits)
TLS_AES_256_GCM	384	256	640

5.3. Confidentiality and encryption overhead (PDPL Article 14)

PDPL Article 14 mandates the implementation of technical measures to protect personal data from unauthorized disclosure. Confidentiality was assessed by inspecting encrypted traffic using PCAPdroid. The captured HTTPS traffic confirmed the use of TLS 1.3 encryption on port 443, with no plain-text payloads observed.

The deployment of strong cryptographic primitives, including AES-256-GCM and SHA-384, ensured a high security level in compliance with PDPL confidentiality requirements. Importantly, the latency measurements reported in Section 5.1 indicate that the cryptographic overhead introduced by TLS 1.3 did not result in a significant degradation of system performance. This demonstrates a favorable trade-off between security enforcement and network responsiveness.

5.4. Authentication and signal integrity (Implied compliance)

Authentication and integrity were indirectly assessed through radio signal quality metrics obtained via the NetMonster application. The network exhibited an RSRP of –102 dBm, RSRQ of –11 dB, and an SNR of 8 dB. These values are consistent with stable 5G NSA operation and imply successful EAP-AKA authentication in accordance with 3GPP standards.

From a control and system reliability perspective, stable signal conditions support continuous authentication and session integrity, reducing the likelihood of retransmissions or session drops that could otherwise impact availability. Together with the encryption results, these findings indicate that PDPL-mandated security mechanisms can be maintained without compromising overall network efficiency.

6. Discussion

The results demonstrate that STC's 5G NSA network achieved compliance with Saudi Arabia's PDPL, while maintaining acceptable system performance. The findings highlight important trade-offs between PDPL compliance and network performance, particularly under high traffic load scenarios, which warrant further analysis.

6.1. Trade-offs between compliance and performance

Personal Data Protection Law Articles 3 and 14 emphasize data availability, confidentiality, and integrity as mandatory compliance requirements. Implementing these requirements, particularly through encryption (TLS 1.3) and authentication (EAP-AKA), introduces processing overhead that can impact real-time network performance under high traffic loads.

6.1.1. Latency vs. security

During busy hours or under high traffic conditions, the signaling and processing demands of cryptographic operations (e.g., TLS handshakes, key generation) can result in increased latency and jitter variability. For example, RTT measurements, which averaged 35 ms under normal conditions, may exceed 50 ms during congestion, potentially violating latency thresholds for certain latency-sensitive applications such as remote surgery or financial transactions. Additionally, forward secrecy in TLS 1.3 mandates frequent session key exchanges, which can amplify signaling delays under heavy load.

6.1.2. Authentication vs. availability

EAP-AKA authentication, crucial to compliance with PDPL Article 3, ensures session-level integrity but adds significant overhead, especially during reauthentication events in congested networks. This overhead can lead to longer attachment times, which may disrupt real-time applications like video conferencing or cloud gaming.

6.1.3. Jitter and quality of service

High traffic load exacerbates jitter (17.2 ms under normal conditions in this study) due to packet queuing delays and retransmissions, which undermine quality of service guarantees. As jitter increases, real-time applications experience performance degradation, even if security measures satisfy confidentiality and integrity requirements.

6.2. Implications for privacy-enhancing technologies

Privacy-enhancing technologies (PETs) are becoming an essential part of compliance in data-intensive networks such as 5G. The World Economic Forum highlights how PETs, including secure multi-party computation and federated learning, enable organizations to use sensitive data securely under rigorous data protection regulations. These approaches specifically address privacy and compliance risks inherent in distributed digital ecosystems.

6.3. Mitigation strategies for balancing compliance and performance

Efforts to address these trade-offs can focus on adaptive, traffic-aware optimization strategies[38]:

i Dynamic resource allocation: Using network slicing and intelligent traffic prioritization (e.g., prioritizing critical data flows while delaying non-essential traffic) can ensure compliance during peak congestion periods.

ii Lightweight cryptographic protocols: Adopting optimized encryption algorithms, such as ChaCha20, in latency-sensitive environments can reduce cryptographic overhead while maintaining a strong security posture.

iii Periodic reauthentication optimization: Leveraging reauthentication reduction mechanisms, such as cached session keys, can mitigate EAP-AKA overhead during periods of high network load.

iv Edge computing and caching: Deploying decentralized edge servers for local session handling can offload cryptographic and authentication processing from the core network, minimizing latency impacts.

While these strategies enhance performance under load, ensuring alignment with PDPL requirements remains essential. A trade-off exists between implementing lightweight mechanisms and satisfying the strict confidentiality and integrity requirements mandated by Articles 3 and 14. Future deployments must adopt optimization frameworks that prioritize compliance dynamically while adapting to real-time traffic conditions.

6.4. Generality of results and cross-operator applicability

This study evaluated PDPL compliance on STC's 5G NSA network in Riyadh, which serves as a representative case study for compliance testing in Saudi Arabia. While STC is the largest telecommunications operator in the Kingdom, the results may share certain limitations in generalizability to other Saudi 5G networks, such as those deployed by Mobily and Zain KSA.

STC's network utilizes a specific NSA architecture, including LTE Band 3 (1,800 MHz) as an anchor for 5G NR layers. This configuration, combined with off-peak testing conditions and device-specific behavior (HONOR X7b), may differ slightly from the infrastructure or deployment scenarios employed by other operators. For

instance, Mobily has implemented different anchor bands and regional coverage strategies that might yield variations in latency, jitter, and signal quality metrics. Similarly, Zain KSA's future SA 5G deployments are expected to exhibit distinct characteristics that diverge from the NSA configurations evaluated here.

However, the broader PDPL compliance framework, including the encryption, authentication, and availability requirements mandated under Articles 3, 10, 14, and 28, is applicable across all operators in Saudi Arabia. The testing methodology demonstrated in this study can be extended to other networks for evaluating compliance performance. This is particularly true for fundamental encryption mechanisms (e.g., TLS 1.3) and authentication protocols (e.g., EAP-AKA) mandated by both national policies and 3GPP standards, which are implemented uniformly across operators.

Future work should include cross-operator testing to validate these trends, ensuring that compliance performance is consistent under varied deployments, configurations, and device types. A comparative analysis between operators would also provide deeper insights into how network-specific factors influence PDPL compliance.

7. Comparative legal analysis

This section provides a comparative analysis of Saudi Arabia's PDPL, enacted in 2023, against three prominent international data protection frameworks: the European Union's GDPR, implemented in 2018; Singapore's Personal Data Protection Act (PDPA), enacted in 2012 and amended in 2020; and the United Arab Emirates' Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (UAE PDPL). All four frameworks aim to protect personal data in an era of advanced telecommunications, but they differ in scope, enforcement mechanisms, technical prescriptiveness, and alignment with cultural and technological contexts. **Table 4** summarizes the core distinctions across all four regimes.

Several key distinctions emerge from this comparison. In terms of scope and jurisdiction, PDPL targets Saudi residents with extraterritorial provisions aligned with Vision 2030's emphasis on local data governance,[1] while GDPR extends globally to any entity processing European Union residents' data, and both the UAE PDPL and Singapore's PDPA adopt intermediate positions with varying degrees of extraterritorial reach.

Regarding consent, PDPL's Article 10 mandates explicit consent aligned with Islamic principles of individual autonomy,[4] while GDPR offers greater flexibility through opt-out and legitimate interest bases, and Singapore's PDPA introduces deemed consent provisions suited for IoT-intensive environments.

On security and technical standards, PDPL is notably prescriptive by explicitly mandating encryption under Article 14, providing clear guidance for 5G operators. In contrast, GDPR, PDPA, and the UAE framework adopt principle-based or risk-based approaches that afford operators greater flexibility but may introduce ambiguity in compliance verification for high-speed 5G environments.

Enforcement mechanisms vary significantly. GDPR's turnover-based fines (up to EUR 20 million or 4% of global turnover) create the strongest deterrent for multinational operators, while Singapore's 2020 amendment substantially increased its penalty ceiling. The UAE's inclusion of criminal penalties adds an additional enforcement dimension. PDPL's SAR 5 million cap is meaningful for local operators but may require upward revision as Saudi Arabia's 5G ecosystem becomes increasingly integrated with global networks.[3]

The absence of explicit data portability provisions in PDPL, compared to GDPR's mandatory portability right and Singapore's phased introduction, represents a gap for 5G IoT ecosystems where interoperability across service providers is critical. Similarly, cross-border data transfer provisions differ in stringency, with PDPL requiring SDAIA approval under Article 28, GDPR employing adequacy decisions and standard contractual clauses, and PDPA and the UAE framework requiring comparable or adequate protection in receiving jurisdictions.

These cross-regime comparisons reveal that while PDPL provides a robust foundation for domestic 5G compliance, its alignment with Islamic privacy principles and national priorities makes it particularly effective for Saudi networks like STC's NSA mode as tested in this study. However, GDPR's global scope, Singapore's pragmatic business-oriented approach, and the UAE's regional alignment offer complementary lessons for scalability and interoperability. Future PDPL amendments could incorporate GDPR's portability provisions, Singapore's deemed consent mechanisms for IoT contexts, and the UAE's criminal penalty provisions to address 5G's evolving risks

Table 4. Comparative data protection framework analysis for 5G compliance

Aspect / Framework	Details
Scope	PDPL: Saudi residents, extraterritorial GDPR: EU residents, global reach PDPA: Singapore-based organizations UAE: UAE residents, extraterritorial
Consent	PDPL: Art. 10, explicit consent GDPR: Art. 6–7, explicit + opt-out PDPA: Consent with deemed exceptions UAE: Explicit, legitimate interest
Security	PDPL: Art. 14, TLS 1.3 mandated GDPR: Art. 32, risk-based measures PDPA: Reasonable arrangements UAE: Appropriate measures
DPIA	PDPL: Required (SDAIA, 2023) GDPR: Required (Art. 35) PDPA: Encouraged, not required UAE: Required for high-risk
Fines	PDPL: Up to SAR 5M GDPR: Up to EUR 20M or 4% turnover PDPA: Up to SGD 1M or 10% turnover UAE: Up to AED 2M; criminal possible
Portability	PDPL: Not explicit GDPR: Art. 20, mandatory PDPA: Phased introduction (2020) UAE: Recognized as a right
Cross-border	PDPL: Art. 28, SDAIA approval GDPR: Art. 44–49, adequacy decisions PDPA: Comparable protection required UAE: Adequate protection or consent
Authority	PDPL: SDAIA GDPR: National DPAs PDPA: PDPC UAE: UAE Data Office

Abbreviations: DPIA: Data protection impact assessment; GDPR: General Data Protection Regulation; PDPA: Personal Data Protection Act; PDPL: Personal Data Protection Law; UAE: United Arab Emirates.

such as network slice vulnerabilities and cross-border roaming security, ensuring robust compliance as Saudi Arabia integrates with global and regional digital markets under Vision 2030.

8. Future work

This section outlines proposed research to explore the SA mode of STC's 5G network, which operates independently of 4G LTE anchors, offering potential enhancements in performance and compliance with the PDPL in Saudi Arabia. Unlike the NSA mode evaluated in this study, SA mode promises ultra-low latency (1–4 ms), higher throughput, and advanced features such as network slicing and edge computing, which are critical for PDPL Article 3 (data availability) and Article 14 (security measures) in emerging applications like smart cities and telemedicine.[1] As SA mode deployment is still in its infancy in Riyadh, this section details a future testing framework, anticipated metrics, and collaboration strategies to validate its compliance potential.

Future testing outlines proposed use of advanced tools commonly employed by mobile operators, including Keysight Nemo Analyze for signal quality, EXFO Xtract for latency and throughput analysis, and Rohde & Schwarz PRISMON for security monitoring. Signal quality outlines proposed assessment using the RSRP formula, with details provided alongside:

$$RSRP_{\text{dBm}} = -P_{\text{rx}} + G_{\text{ant}}$$

where P_{rx} is the received power (in dBm), and G_{ant} is the antenna gain (in dB). Preliminary simulations suggest RSRP values, as shown in **Table 5**, will vary across urban and suburban locations, with Riyadh urban estimated at –95 dBm received power and 2 dB gain, yielding an RSRP of –93 dBm.

Latency and throughput testing will target RTT < 10 ms and throughput > 100 Mbps, using the throughput formula:

$$Throughput_{\text{Mbps}} = \frac{8 \cdot \text{Data Size (MB)}}{\text{Transfer Time (s)}} \quad (7)$$

Based on NSA trends (5.6 ms RTT), SA is expected to achieve an average RTT of 4 ms, enhancing PDPL Article 3 availability for real-time data access. **Table 6** projects performance metrics under varied conditions.

Security testing outlines proposed extension to SA's 5G core, verifying end-to-end TLS 1.3 encryption and EAP-AKA authentication across sliced networks, addressing PDPL Article 14 confidentiality. Additional security aspects outline proposed exploration including mobile network signaling security (e.g., GPRS tunneling protocol for user data tunneling, packet forwarding control protocol for user plane control, and service-based architecture for service-based architecture Application Programming Interface), which are vulnerable to session hijacking or Application Programming Interface abuse. Mobile network radio access network (RAN) security, such as the RAN Security Gateway, outlines proposed assessment to secure backhaul traffic with IPsec, preventing over-the-air attacks. Carrier-grade network address translation (NAT) solutions (e.g., NAT44 for IPv4 conservation, NAT64 for IPv6-IPv4 transition) outline proposed testing for address management and traffic security, aligning with PDPL's data protection requirements. Improved monetization through gateway interface firewall services outlines proposed evaluation for N6 interface security, while telco applications and Application Programming Interface security (e.g., OAuth2 validation) outline proposed probing for service-based architecture vulnerabilities. Finally, virtualization and orchestration security (e.g., network functions virtualization, virtual network functions, management and orchestration) outlines proposed addressing of risks in dynamic slicing.

Challenges outline proposed inclusion of limited SA coverage in Riyadh, requiring partnerships with STC for test site access and authentication logs. Unrooted device limitations outline proposed necessity of custom firmware or emulators, while deep security testing (e.g., GPRS tunneling protocol, packet forwarding control protocol, RAN SecGW) exceeds mobile app capabilities, requiring lab tools like Wireshark or operator collaboration. Operator and research -grade tools such as Keysight Nemo Analyze, EXFO Xtract, and Rohde & Schwarz PRISMON outline proposed use to provide comprehensive insights into signaling, RAN, NAT, and orchestration security, though their deployment will depend on STC's infrastructure access. Collaboration with CST outlines proposed ensuring alignment with national 5G plans, with testing proposed to begin in Q2 2026. This future work outlines proposed bridging of NSA findings with SA's advanced security and performance potential, enhancing PDPL compliance as Saudi Arabia advances its 5G ecosystem under Vision 2030.

Machine learning-assisted optimization offers a promising pathway to enhance both security and performance in this context. By analyzing real-time network telemetry, machine learning models can detect anomalous traffic patterns, predict congestion or security threats, and enable proactive control actions. Prior studies on 5G anomaly detection have demonstrated that machine learning-based approaches can reduce security-induced performance degradation and improve latency stability under attack or misconfiguration scenarios. Applied to PDPL compliance, such models could dynamically balance encryption overhead, authentication frequency, and resource allocation to sustain regulatory adherence while minimizing latency impact.

Looking ahead to 6G, where networks are expected to support massive device densities, artificial intelligence-native architectures, and ultra-reliable low-latency communications, the integration of legal constraints into optimization and control frameworks will become increasingly important. The findings of this study suggest that regulatory compliance should be treated not as a static checklist, but as an adaptive system property governed by continuous monitoring, optimization, and control. This perspective positions data protection laws such as PDPL as integral design parameters in future intelligent communication systems rather than external constraints imposed post-deployment.

Table 5. Standalone mode signal quality (projected)

Location	$P_{\mathbf{rx}}$ **(dBm)**	$G_{\mathbf{ant}}$ **(dB)**	$RSRP_{\mathbf{dBm}}$
Riyadh urban	–95	2	–93
Riyadh suburban	–100	2	–98
Olaya district	–92	2	–90

Table 6. Standalone mode performance metrics (projected)

Test case	**Metrics**	**RTT (ms)**	**Compliance**
Urban high load	Throughput: 150 Mbps	4.2	Yes
Suburban low load	Throughput: 120 Mbps	3.8	Yes
Peak hour	Throughput: 95 Mbps	5.5	No (Throughput)

Abbreviations: RTT: Round-trip time.

9. Conclusion

This study demonstrates that STC NSA network achieves compliance with Saudi Arabia's PDPL while maintaining acceptable system performance. Empirical measurements confirm that regulatory requirements for data availability, confidentiality, and integrity can be satisfied without introducing prohibitive latency or instability, even under the security mechanisms mandated by PDPL. These findings indicate that data protection compliance and network performance are not mutually exclusive, but rather can be jointly addressed through careful system design.

From an optimization and control perspective, the results highlight the importance of treating regulatory requirements as operational constraints within network performance management. Metrics such as latency, jitter, and authentication stability can be viewed as control variables that must be optimized under confidentiality and integrity constraints imposed by data protection laws. This framing supports the development of adaptive network control strategies that dynamically balance security overhead with service quality.

As networks evolve toward 5G SA and future 6G architectures, the complexity of compliance-aware network management will increase due to features such as network slicing, ultra-low-latency services, and massive device connectivity. Future research should therefore focus on performance optimization and adaptive control mechanisms that incorporate legal constraints directly into network decision-making processes. In particular, machine learning-assisted approaches offer promising opportunities for real-time anomaly detection, predictive performance optimization, and automated compliance enforcement.

Overall, this work positions PDPL compliance not as a static regulatory obligation, but as a dynamic system property that can be monitored, optimized, and controlled. By bridging legal requirements with measurable network performance, the study contributes a foundation for constraint-based network design approaches that align data protection objectives with the operational goals of next-generation communication systems.

Acknowledgments

All authors of this article would like to thank the Governance and Policy Design Research Lab (GPDRL) of Prince Sultan University (PSU) for financial and academic support to conduct this research and publish it in sustainability journal.

Funding

The study was funded by the Governance and Policy Design Research Lab (GPDRL) of Prince Sultan University (PSU).

Conflict of interest

The authors declare they have no competing interests.

Author contributions

Conceptualization: All authors
Formal analysis: Eyad Al Samara
Investigation: Eyad Al Samara
Methodology: All authors
Writing – original draft: Eyad Al Samara
Writing–review & editing: All authors

Availability of data

Not applicable.

AI tools statement

All authors confirm that no AI tools were used in the preparation of this manuscript.

References

1. Saudi Data and Artificial Intelligence Authority. *Personal Data Protection Law*. Saudi Data and Artificial Intelligence Authority; 2021. Accessed February 28, 2026. Available at: https://sdaia.gov.sa/en/SDAIA/about/Pages/RegulationsAndPolicies.aspx
2. Saudi Data and Artificial Intelligence Authority. *Implementing Regulations of the Personal Data Protection Law*. Saudi Data and Artificial Intelligence Authority; 2023. Accessed September 3, 2025. Available at: https://sdaia.gov.sa/en/SDAIA/about/Documents/ImplementingRegulation.pdf
3. PwC Middle East. *Guide to the Saudi Personal Data Protection Law*. PwC Middle East; 2023. Accessed February 28, 2026. Available at: https://www.pwc.com/m1/en/blogs/pdf/ksa-personal-data-protectionlaw-series-part-1.pdf
4. Sarabdeen J, Ishak MM. Compliance of Saudi Arabian Personal Data Protection Law 2021 to Islamic principles of privacy. *Migration Lett.* 2024;21(4):726-737.
5. National Data Management Office. *Data Management and Personal Data Protection Standards, Version 1.5*. Saudi Data and Artificial Intelligence Authority; 2021. Accessed February 28, 2026. Available at: https://sdaia.gov.sa/ndmo/Files/PoliciesEn001.pdf
6. Saudi Data and Artificial Intelligence Authority. *Elaboration and Developing Privacy Policy Guideline, Version 1.0*. Saudi National Data Governance Platform; 2024. Accessed February 28, 2026. Available at: https://dgp.sdaia.gov.sa/wps/wcm/connect/3125da48-43dd-46bc-9156-1f7b91ab8f54/Elaboration+and+Developing+Privacy+Policy+Guideline.pdf?MOD=AJPERES
7. Maganti MR, Rao KR. Enhancing 5G Core Network Performance through Optimal Network Fragmentation and Resource Allocation. *Eng Technol Appl Sci Res*. 2024;14(3):14588-14593. https://www.doi.org/10.48084/etasr.7235
8. Yuan Q, Liu Z, Jiang X, Hu H, Yang Y, Li J. Allocation of computing resources based on multi-objective strategy and performance improvement in 5G networks. *Computer Communications*. 2025;238:108197. https://www.doi.org/10.1016/j.comcom.2025.10819
9. Pazienza A, Bozzolo L, Mancuso D, Rossi M, Aloi G, Gravina R. Optimizing 5G Networks for Low-Latency Communication: A Reinforcement Learning-Based Approach. *Procedia Computer Science*. 2025;253:1780-1789. https://www.doi.org/10.1016/j.procs.2025.01.240
10. Kumar A, Singh P, Kamble DP, Singh I. Hybrid cryptographic approach for strengthening IoT and 5G/B5G network security. *Sci Rep*. 2025;15(1). https://www.doi.org/10.1038/s41598-025-21861-2
11. Alkhamsi NN, Alqahtani SS. Compliance Framework for Personal Data Protection Law Standards. *IJACSA*. 2024;15(7). https://www.doi.org/10.14569/ijacsa.2024.0150751
12. Alsamara T, Farouk G. Artificial Intelligence and Legal Transparency: A Comparative Analysis between Public and Private Law. *JoPH*. 2025;5(1). https://www.doi.org/10.63332/joph.v5i1.685
13. Ko Y, Pawana IWAJ, Won T, Astillo PV, You I. Toward an Era of Secure 5G Convergence Applications: Formal Security Verification of 3GPP AKMA with TLS 1.3 PSK Option. *Applied Sciences*. 2024;14(23):11152. https://www.doi.org/10.3390/app142311152
14. Al-Khalifa H, Mashaabi M, Al-Yahya G, Alnashwan R. The Saudi Privacy Policy Dataset. *arXiv*. 2023. https://www.doi.org/10.48550/ARXIV.2304.02757
15. Madkhali AM, Bouri HA, Alotaibi FOE, et al. Potential Health Implications of Fifth Generation (5G) Wireless Communication Technology. *Saudi J Med Public Health*. 2024;1(1):94-105. https://www.doi.org/10.64483/20251125
16. Communications, Space and Technology Commission. *Telecommunications and Information Technology Bylaw*. Communications, Space and Technology Commission; 2025. Accessed September 3, 2025. Available at: https://www.cst.gov.sa/en/regulations
17. Alhazmi A, Daghistani A. Privacy practices of popular websites in Saudi Arabia. *J Umm Al-Qura Univ EngArchit*. 2024;16(1):19-29. https://www.doi.org/10.1007/s43995-024-00085-x
18. Alkhamsi, N. N., & Alqahtani, S. S. Data privacy governance in data management ecosystems: a compliance framework for PDPL standards. In: Abd El-Latif AA, ElAffendi MA, AlShara MA, Maleh Y, eds. *Cybersecurity, Cybercrimes, and Smart Emerging Technologies*. CRC Press; 2025:213-226. https://www.doi.org/10.1201/9781003614197
19. Sabur A, Showail AJ. Nudging Data Privacy of Mobile Health Applications in Saudi Arabia. *International Journal of Information Security and Privacy*. 2024;18(1):1-19. https://www.doi.org/10.4018/ijisp.345647
20. Madhusudhanan S, Jose AC. Privacy preservation techniques through data lifecycle: A comprehensive literature survey. *Computers Security*. 2025;155:104473. https://www.doi.org/10.1016/j.cose.2025.104473
21. Oluchukwu M, Oluoha, Odeshina A, et al. A Privacy-First Framework for Data Protection and

Compliance Assurance in Digital Ecosystems. *IRE Journals*. 2023;7(4).
22. Alnashwan R, Gope P, Dowling B. Privacy-Aware Secure Region-Based Handover for Small Cell Networks in 5G-Enabled Mobile Communication. *IEEE TransInformForensic Secur*. 2023;18:1898-1913. https://www.doi.org/10.1109/tifs.2023.3256703
23. Ain N, Waqar M, Bilal A, et al. A Novel Approach Based on Quantum Key Distribution Using BB84 and E91 Protocol for Resilient Encryption and Eavesdropper Detection. *IEEE Access*. 2025;13:32819-32833. https://www.doi.org/10.1109/access.2025.3539178
24. Sajid M, Malik KR, Khan AH, Bilal A, Alqazzaz A, Darem AA. Advanced multilayer security framework: integrating AES and LSB for enhanced data protection. *J Supercomput*. 2025;81(17). https://www.doi.org/10.1007/s11227-025-08093-x
25. European Union Agency for Cybersecurity (ENISA). *GDPR-Compliant 5G Security*. European Union Agency for Cybersecurity; 2022. Accessed: Feb. 28, 2026. Available at: https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing
26. Abdullah Alsadhan A. A Survey of Security Threats and Challenges Related To 5G Networks in Saudi Arabia. *QAJ*. 2025;5(3):474-501. https://www.doi.org/10.48161/qaj.v5n3a1849
27. Bartock M. *5G Network Security Design Principles: Design Principles*: National Institute of Standards and Technology; 2025. https://www.doi.org/10.6028/nist.cswp.36e.ipd
28. Wang Y, Wang R, Liu X, et al. A Framework for TLS Implementation Vulnerability Testing in 5G. In: *Lecture Notes in Computer Science*. Springer Nature Switzerland; 2023:284-298. https://www.doi.org/10.1007/978-3-031-41181-6_16
29. Ericsson. *Elevating 5G with Differentiated Connectivity: Saudi Arabia*. Ericsson ConsumerLab Report; 2025. Accessed: Jun. 2, 2026. Accessed February 28, 2026.Available at:
30. Lastre JK, Ko Y, Kwon H, You I. Evaluating Transport Layer Security 1.3 Optimization Strategies for 5G Cross-Border Roaming: A Comprehensive Security and Performance Analysis. *Sensors*. 2025;25(19):6144. https://www.doi.org/10.3390/s25196144
31. nPerf. *nPerf Speed Test 4G 5G WiFi & Maps. Mobile application*. nPerf; 2025. Accessed: Feb. 28, 2026. Available at: https://play.google.com/store/apps/details?id=com.nperf.tester
32. PCAPdroid. *PCAPdroid - Network Monitor*. Mobile application. Emanuele Faranda; 2025. Accessed: Feb. 28, 2026. Available at: https://play.google.com/store/apps/details?id=com.emanuelef.remote capture.
33. NetMonster. *NetMonster*. Mobile application. Michal Mroček; 2025. Accessed: Feb. 28, 2026. Available at: https://play.google.com/store/apps/details?id=cz.mroczis.netmonster
34. Olomina J. AI-driven compliance monitoring frameworks for automated detection and classification of data privacy violations in hybrid infrastructures. *Int J Sci Res Arch*. 2025;16(3):202-208. https://www.doi.org/10.30574/ijsra.2025.16.3.2541
35. Pavani GK, Veeramallu B. Hybrid Machine Learning Framework for Anomaly Detection in 5G Networks. *JISEM*. 2025;10(32s):733-739. https://www.doi.org/10.52783/jisem.v10i32s.5406
36. Samara EA, Akamine C. Identifying Key Parameters Affecting Energy Efficiency in 5G Networks Using Machine Learning. In: *2025 Interdisciplinary Conference on Electrics and Computer (INTCEC)*. IEEE; 2025:1-5. https://www.doi.org/10.1109/intcec65580.2025.11256175
37. World Economic Forum. *How Privacy Enhancing Technologies Impact Business, Individuals, and Society*. World Economic Forum; 2023. Accessed: Jun. 2, 2026. Available at: https://www.weforum.org/stories/2023/10/the-impact-ofprivacy-enhancing-technologies-pet-on-business-individuals-and-society
38. Usman HM, Imran A, Bilal A, Garayev M, Fathi H, Dhelim S. Resource-Limited Skew Estimation and Correction (RLSEC) for Edge Devices in Delay Non-Tolerant Networks. *IEEE Access*. 2024;12:159597-159610. https://www.doi.org/10.1109/access.2024.3469581

Tareck Alsamara *is an Associate Professor of Private Law at Prince Sultan University, Saudi Arabia. He previously taught at Syrian and French universities and practiced law with the Damascus Bar Association. His research focuses on private law, technology law, and data protection, with publications in English, Arabic, and French.*
https://orcid.org/0000-0003-0202-0024

Eyad Al Samara *is a Senior Researcher at Mackenzie Presbyterian University, Brazil, and Professor at ESTIAM School of Informatics, France. He has 14 years of industrial experience with Huawei Technologies, specializing in telecommunications, 5G, mobile networks, radio access technologies, and machine learning applications for telecommunications systems.*
https://orcid.org/0009-0007-6553-300X

An International Journal of Optimization and Control: Theories & Applications
(https://accscience.com/journal/ijocta)