TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 24, No. 5, October 2026, pp. 1480∼1491
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v24i5.27849

Virtualized evolved packet core deployment strategies in emerging Palestinian mobile networks

Saed Tarapiah[1], Shadi Atalla[2], Khawla Hafiz Daraghme[3]
[1]Telecommunication Engineering Department, An–Najah National University, Nablus, Palestine
[2]College of Engineering and Information Technology, University of Dubai, Dubai, United Arab Emirates
[3]Ooredoo Palestine, Ramallah, Palestine

Article Info

Article history:

Received Feb 3, 2026
Revised Jun 21, 2026
Accepted Jun 30, 2026

Keywords:

Emerging mobile networks
Deployment strategy
KPI-based weighted scoring
Mobile core network virtualization
Multi-criteria decision analysis
Network function virtualization
Virtualized evolved packet core

ABSTRACT

Mobile operators in emerging markets face rising data demand under revenue, infrastructure, regulatory, and investment constraints. Network function virtualization (NFV) enables evolved packet core (EPC) modernization, but operators must determine which deployment model provides the best strategic and operational fit. This paper examines EPC virtualization as an operator-level deployment-selection problem using Palestine as a case study. A context-specific decision framework integrates operator readiness, stakeholder-derived key performance indicator (KPI) weights, deployment-model ratings, capital expenditure (CapEx) / operating expenditure (OpEx) analysis, analytic hierarchy process (AHP) consistency checking, and technique for order of preference by similarity to ideal solution (TOPSIS)-style robustness validation. Five alternatives are compared under the same operator scenario: owned legacy EPC, owned NFV / virtualized evolved packet core (vEPC), network functions virtualization infrastructure as a service (NFVIaaS), virtual network platform as a service (VNPaaS), and virtual network service as a service (VNSaaS). The novelty lies in linking multi-criteria scoring to local regulatory, infrastructure, security, supply-chain, and business constraints rather than applying generic weighted ranking alone. Scenario-based technical validation examines latency / quality of service (QoS) exposure, scalability, recovery, elasticity, and observability. The results indicate that fully owned vEPC provides the strongest overall fit when service control, quality, implementation constraints, and long-term operational efficiency are jointly considered.

Corresponding Author:

Saed Tarapiah
Telecommunication Engineering Department, An–Najah National University
Nablus, Palestine
Email: s.tarapiah@najah.edu

1. INTRODUCTION

Mobile operators in emerging markets must expand mobile broadband, internet of things (IoT), machine-to-machine (M2M) , cloud, and low-latency services while facing revenue pressure, spectrum limitations, infrastructure restrictions, and limited investment capacity. Legacy enables evolved packet core (EPC) deployments, which are tightly coupled to proprietary hardware, are therefore increasingly difficult to scale economically. Network function virtualization (NFV) offers a modernization path by decoupling mobile-core functions from dedicated appliances and supporting virtualized or cloud-based deployment of EPC functions [1]-[5]. Recent work confirms the importance of software-defined networking (SDN) / NFV integration, cloud-native core functions, service-based architectures, and virtualized core investment for 5G evolution [6]-[10].

The central problem for constrained operators is not only whether EPC virtualization is feasible, but which deployment and service model should be selected under technical, business, regulatory, and operational constraints. This issue is critical in Palestine, where operators face infrastructure restrictions, supply-chain limitations, regulatory uncertainty, and external competition. Existing studies mostly optimize or validate selected virtualized/cloud-native architectures through resource allocation, testbeds, observability, slice federation, security, or orchestration [11]-[18]. Fewer studies provide an operator-level decision framework that compares alternative EPC deployment models under one emerging-market scenario and translates the ranking into cost, governance, security, regulatory, and operational-control implications.

Accordingly, the research question is: *Which EPC deployment model provides the most suitable balance of cost, quality, time to market, security, regulatory alignment, value proposition, and operational complexity for a Palestinian mobile operator operating under emerging-market constraints?* The novelty is not a new generic multi-criteria decision analysis (MCDA) algorithm; rather, it is the adaptation of multi-criteria scoring into a deployment-specific EPC virtualization decision framework that links stakeholder priorities, analytic hierarchy process (AHP)-supported key performance indicator (KPI) weighting, technique for order of preference by similarity to ideal solution (TOPSIS)-style robustness checking, total cost of ownership (TCO) estimation, and scenario-based technical validation to local operating constraints.

The main contributions are: (i) formulating EPC virtualization as a deployment-selection problem; (ii) proposing a context-aware decision framework; (iii) comparing owned legacy EPC, owned NFV / virtualized evolved packet core (vEPC), network functions virtualization infrastructure as a service (NFVIaaS), virtual network platform as a service (VNPaaS), and virtual network service as a service (VNSaaS) with unified KPIs; (iv) clarifying how this work differs from NFV studies focused mainly on technical optimization or testbed validation; and (v) showing why owned vEPC can outperform lower-capital expenditure (CapEx) outsourced models when quality of service (QoS) governance, operational control, security accountability, and long-term operating expenditure (OpEx) are jointly considered.

2. COMPREHENSIVE THEORETICAL BASIS AND RELATED WORK

2.1. Legacy EPC and virtualized EPC background

The EPC is the internet protocol (IP)-based mobile-core architecture responsible for mobility management, session control, policy enforcement, subscriber data handling, and packet-gateway functions. Its main logical elements include the mobility management entity (MME), serving gateway (SGW), packet data network gateway (PGW), policy and charging rules function (PCRF), and home subscriber server (HSS) [19]. In conventional operator deployments, these functions are usually implemented through appliance-centric and vendor-specific platforms. Such platforms are stable and operationally familiar, but they are less adaptable to fast traffic growth, service diversification, and rapid capacity expansion. Figure 1 illustrates the conventional EPC logical structure used as the baseline in this study.

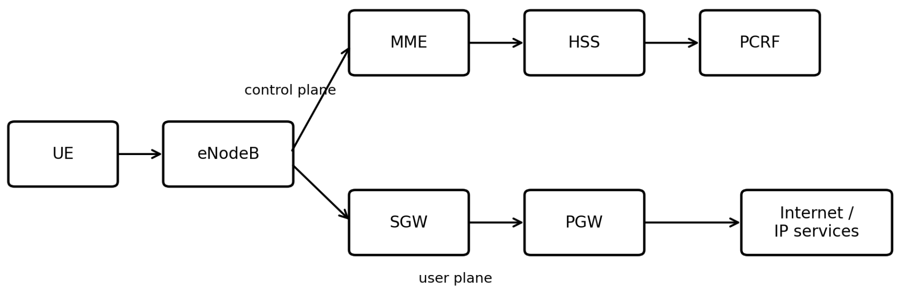


Figure 1. Conventional legacy EPC architecture used as the baseline deployment model

NFV changes this model by decoupling network functions from dedicated hardware and enabling EPC functions to run as VNFs over a shared NFV infrastructure (NFVI), governed by management and orchestration functions [5], [20]. This separation allows operators to pool compute resources, automate lifecycle operations, scale VNFs according to traffic demand, and reduce dependence on single-purpose appliances. However, the value of NFV depends strongly on the selected deployment model. A model with low initial CapEx may introduce external dependency, weaker observability, stricter service level agreement (SLA) reliance, or regulatory exposure; conversely, an owned model may require higher initial investment but provide stronger long-term control.

2.2. Deployment models considered in this study

Five deployment alternatives are evaluated under one fixed operator scenario. The legacy EPC model represents the baseline appliance-based architecture. Owned NFV/vEPC means that the operator owns and manages the NFVI, VNFs, and lifecycle-control processes. NFVIaaS shifts the infrastructure layer to an external provider while keeping VNF control largely with the operator. VNPaaS provides an integrated virtualized platform on which network services can be deployed. VNSaaS provides the network software as a service and therefore shifts the greatest portion of control to the service provider. Table 1 summarizes the decision relevance of these models.

Table 1. Deployment models and main decision implications

Model	Ownership and control	Main benefit	Main risk
Legacy EPC	Operator owns appliance-based EPC	Familiar operation and direct control	Weak elasticity and high lifecycle cost
Owned NFV/vEPC	Operator owns NFVI, VNFs, and orchestration	Strong control, scalability, and observability	Higher implementation and skill requirements
NFVIaaS	Provider owns infrastructure; operator manages VNFs	Reduced CapEx and infrastructure burden	Provider dependency and cross-domain troubleshooting
VNPaaS	Provider offers virtualized platform	Faster service development and platform abstraction	Reduced control over platform behavior
VNSaaS	Provider offers network software as a service	Minimal initial CapEx and rapid consumption	Highest external dependency and recurring OpEx

2.3. Positioning against existing work

Recent NFV and fifth generation (5G)-core literature can be grouped into four streams. The first stream focuses on cloud-native resource allocation and automation for virtualized or microservice-based cores [11]. The second develops experimental platforms and testbeds for 5G-core deployment, analytics, and observability [12], [14]. The third addresses slice federation, multi-domain orchestration, and cross-administrative-domain service continuity [13]. And the fourth studies energy efficiency, user plane function (UPF) placement, security, and resilience in softwarized cores [15]-[18]. These works improve important mechanisms after a core architecture has already been selected.

The present study addresses a different decision level. It does not propose a new generic optimization algorithm or a single testbed implementation. Instead, it formalizes the earlier operator decision: which EPC deployment model should be selected before implementation under constrained market conditions. This requires simultaneous consideration of technical feasibility, TCO, regulatory exposure, security accountability, troubleshooting autonomy, service control, and provider dependence. Table 2 positions the study against representative recent work.

Table 2. Novelty positioning relative to representative recent NFV/5G-core work

Approach	Primary output	Difference of this study
Cloud-native resource allocation [11]	Allocation policy or resource optimization	This work selects among deployment/service models before resource-optimization policies are applied
5G-core testbeds [12]	Experimental deployment and measurements	This work provides a decision framework; testbeds are future validation instruments for the selected model
Slice federation [13]	Cross-domain slice orchestration	This work determines the baseline EPC/vEPC ownership and service model before slice federation is considered
Energy/UPF studies [15], [16]	Placement and energy-performance tradeoff	This work maps energy and performance implications into operator-level KPIs and TCO interpretation
Observability studies [14]	Monitoring and troubleshooting mechanisms	This work treats observability as a decision criterion affecting model selection and governance

This positioning clarifies the contribution: the weighted scoring, AHP, and TOPSIS components are not presented as new algorithms. They are used as formal instruments inside a context-aware EPC deployment-selection framework. The novelty is therefore methodological and practical: the framework translates the broad

NFV modernization problem into an auditable operator decision process for a constrained emerging-market environment.

3. METHOD

This study uses a case-study-based MCDA design. The scenario is fixed for all alternatives in terms of EPC functional scope, traffic-growth assumptions, regulatory setting, service portfolio, redundancy target, and market constraints. Empirical input was obtained through structured and semi-structured discussions with an anonymized panel of seven experts selected for direct involvement in mobile-core planning, EPC operation, NFV / cloud infrastructure, QoS, security / regulatory compliance, or telecom business strategy are summarized in Table 3. The process had three stages: confirmation of the five deployment alternatives, review of the KPI set, and comparative judgments for KPI weighting and model scoring. Aggregated group judgment was used rather than a single-respondent score.

Table 3. Anonymized expert panel used for KPI elicitation

Background	No.	Evaluation role
Mobile-core / EPC engineering	2	EPC functions, migration feasibility, control / user-plane implications
NFV / cloud infrastructure	1	NFVI, orchestration, virtualization readiness, scalability
Network operations / QoS	2	Availability, SLA assurance, troubleshooting, service continuity
Security / regulatory / governance	1	Compliance, security exposure, data control, regulatory constraints
Business strategy / procurement	1	CapEx/OpEx, vendor dependency, time to market, business value
Total	7	Aggregated expert judgment for weights and scores

AHP is used to formalize expert judgments and reduce subjectivity. For comparison matrix $A = [a_{ij}]$, the weight vector is obtained from:

$$Aw = \lambda_{\max} w, \qquad CI = \frac{\lambda_{\max} - n}{n-1}, \qquad CR = \frac{CI}{RI}. \tag{1}$$

Judgments with unacceptable inconsistency should be reviewed before finalizing the weights [21], [22]. The final KPI weight is calculated as (2).

$$w_k = 0.25b_k + 0.15t_k + 0.60d_k, \tag{2}$$

where b_k, t_k, and d_k are normalized AHP-supported contributions from business-strategy, transformation-trigger, and technical-deployment viewpoints. The coefficients reflect the case-specific importance of technical feasibility, security, operational control, and service continuity, while still incorporating business and transformation drivers.

Each model m is rated against KPI k using $r_{m,k} \in [1, 5]$ and scored as (3).

$$S_m = \frac{\sum_{k=1}^{K} w_k r_{m,k}}{\sum_{k=1}^{K} w_k} \tag{3}$$

A TOPSIS-style robustness check is then applied using a normalized matrix $v_{m,k} = w_k r_{m,k} / \sqrt{\sum_{m=1}^{M} r_{m,k}^2}$, positive/negative ideals A^+ and A^-, distances D_m^+ and D_m^-, and the closeness coefficient:

$$C_m = \frac{D_m^-}{D_m^+ + D_m^-} \tag{4}$$

A higher C_m means the model is closer to the positive ideal and farther from the negative ideal [23].

To preserve reproducibility, the scoring matrix was constrained by four controls. First, all models were evaluated using the same EPC functional scope and the same planning horizon. Second, each KPI was interpreted using a predefined direction: higher values indicate stronger suitability, except for cost and complexity where lower exposure is converted into a higher suitability score. Third, expert disagreement was treated as a trigger for clarification, not as an automatic average when meanings differed. And fourth, cost, governance, security, and technical-performance evidence were cross-checked against the literature to avoid relying solely on expert perception. These controls are summarized in Table 4.

Table 4. Reproducibility and validity controls in the evaluation framework

Control	Purpose
Fixed operator scenario	Ensures that differences among alternatives come from the deployment model, not from changing demand or scope assumptions
Common KPI direction	Converts cost, complexity, security, and QoS criteria into comparable suitability scores
Aggregated expert judgment	Reduces single-respondent bias and forces clarification when interpretations diverge
AHP consistency check	Detects inconsistent pairwise judgments before weights are finalized
TOPSIS robustness check	Tests whether the preferred model remains stable under ideal-solution interpretation
TCO and scenario validation	Adds financial and technical support beyond subjective scoring

4. RESULTS AND DISCUSSION

4.1. Case-study readiness and KPI priorities

The case-study assessment indicates that Wataniya Mobile has strategic interest in EPC virtualization because the transformation is linked to service agility, long-term cost control, improved QoS governance, and preparation for future 4G/5G-oriented core evolution. The operator context also shows that virtualization cannot be evaluated only as a technology-upgrade project. It must be evaluated as a combined technical, financial, regulatory, and operational-control decision.

Stakeholder input emphasized that OpEx reduction and QoS/SLA assurance are the strongest decision drivers. This is consistent with constrained-market economics, where traffic growth increases operating pressure while revenue per unit of traffic may decline. Regulatory-constraint mitigation, operational-complexity reduction, and security control were also prioritized because outsourced models can shift control points outside the operator boundary. Table 5 summarizes the condensed KPI hierarchy used in the final evaluation.

Table 5. Condensed KPI priority structure used in the case study

Rank	KPI group	Decision meaning in the Palestinian operator context
1	OpEx reduction	Long-term sustainability, lifecycle cost control, and operational automation
2	QoS, availability, and SLA assurance	Ability to maintain service quality under growth, failures, and traffic peaks
3	Regulatory-constraint mitigation	Fit with local infrastructure limitations, policy uncertainty, and data-control needs
4	Operational-complexity reduction	Ease of troubleshooting, lifecycle control, process adaptation, and staff readiness
5	Security-threat minimization	Control over sensitive core functions, interfaces, data exposure, and attack surface
6	Time-to-market and value proposition	Ability to launch new services and support digital-transformation objectives
7	CapEx and implementation complexity	Initial affordability, procurement feasibility, deployment risk, and migration effort

The priority structure confirms why the preferred model should not be selected using CapEx alone. The operator needs a model that balances cost, control, QoS, and governance. Therefore, the evaluation gives strong weight to the technical-deployment viewpoint while retaining business-strategy and transformation-trigger dimensions through the AHP-supported weighting model.

4.2. KPI, cost, and deployment-model evaluation

The final KPI set covers OpEx, QoS/availability/SLA assurance, regulatory-constraint mitigation, operational complexity, security control, time to market, value proposition, CapEx, management complexity, implementation complexity, and regulatory compliance. The cost component is modeled as five-year TCO. For deployment model m,

$$CapEx_m = C_m^{HW} + C_m^{SW} + C_m^{NFVI} + C_m^{MANO} + C_m^{INT} + C_m^{MIG} + C_m^{TR} + C_m^{CONT}, \quad (5)$$

$$OpEx_m = \sum_{y=1}^{Y} \left(C_{m,y}^{SUP} + C_{m,y}^{LIC} + C_{m,y}^{ENE} + C_{m,y}^{FAC} + C_{m,y}^{STAFF} + C_{m,y}^{SLA} + C_{m,y}^{NET} + C_{m,y}^{OPS} \right)$$
$$TCO_m = CapEx_m + OpEx_m \quad (6)$$

For service-based alternatives, recurring service cost is represented by (7).

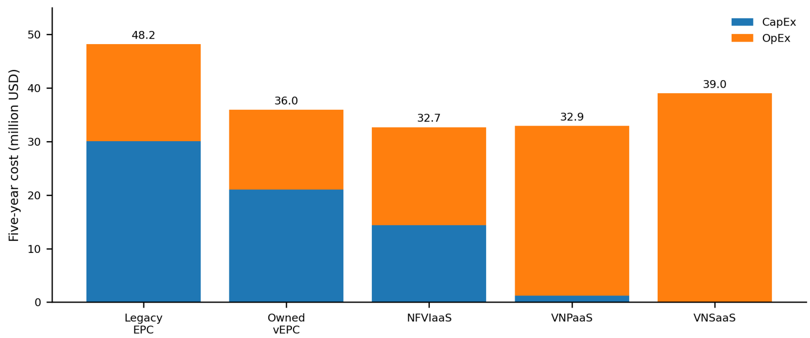
$$C_{m,y}^{SVC} = F_m + \alpha_m D_y + \beta_m R_y + \gamma_m A_y, \quad (7)$$

where F_m is the fixed annual charge, D_y is capacity demand, R_y is redundancy level, and A_y is the SLA class. Cost assumptions combine operator planning inputs, aggregated commercial estimates, NFV architecture assumptions, expert judgment, energy/performance literature, and market benchmarks [15], [24]-[26]. Public market reports are used as secondary trend checks, not direct price inputs [9], [10]. Table 6 summarizes the major cost components and sources used to make the calculation reproducible without disclosing confidential vendor quotations.

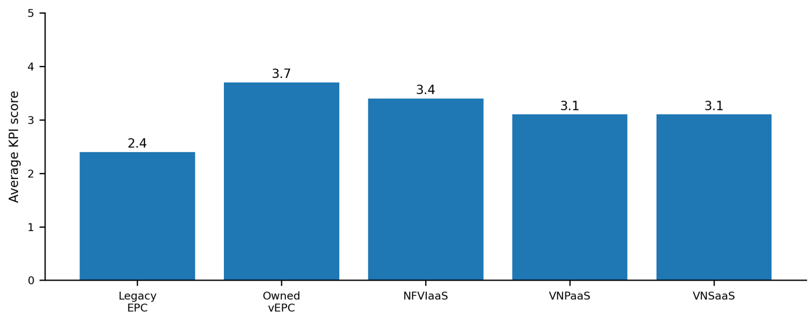
Table 6. Cost model assumptions and estimation basis

Cost element	Included items	Estimation basis
Hardware/NFVI CapEx	EPC appliances, commodity servers, storage, switching, virtualization layer	Operator planning input, aggregated vendor estimates, NFV architecture assumptions [5], [24]
Software/management and orchestration (MANO) CapEx	EPC/vEPC licenses, VNF packages, orchestration, integration middleware	NFV deployment literature and operator technical assumptions [5], [6]
Migration/training	Design, testing, migration planning, acceptance, staff training	Expert-panel judgment and transformation assumptions [27]
Recurring licenses/support	Subscriptions, managed-service fees, hardware/software support	Aggregated commercial estimates and market benchmarks [9], [10]
Energy/facilities/operations	Power, cooling, floor space, monitoring, backup, patching, troubleshooting	Energy/performance and lifecycle-management literature [15], [26]
SLA/provider dependency	Connectivity, redundancy premiums, cross-domain support, external escalation	Service-model assumptions and expert judgment [24], [25]

Figure 2 visualizes the cost and final-score results. The visual comparison shows that service-based options reduce initial CapEx, whereas owned NFV/vEPC provides the strongest final score and the lowest five-year OpEx as shown in Table 7 and Figures 2(a) and (b), while Table 8 summarizes the comparativeevaluation of each deployment model across the complete decision KPI set. The results in Table 7 show that owned NFV/vEPC has the highest overall score and the lowest OpEx, although it is not the lowest-CapEx option. NFVIaaS and VNPaaS are attractive for capital-constrained scenarios, but they introduce stronger provider dependency and cross-domain troubleshooting/SLA exposure. VNSaaS minimizes initial CapEx but accumulates high recurring OpEx and weakens direct EPC performance governance. Legacy EPC remains familiar and controlled but lacks elasticity and produces the weakest overall case fit.



(a)



(b)

Figure 2. Cost and final KPI-score results for: (a) five-year TCO structure and (b) final KPI score ranking

Table 7. Five-year CapEx, OpEx, TCO, and final core

Model	CapEx (K USD)	OpEx (K USD)	TCO (K USD)	Score
Legacy EPC	30,097	18,118	48,215	2.4
Owned NFV/vEPC	21,016	14,950	35,966	3.7
NFVIaaS	14,353	18,339	32,692	3.4
VNSaaS	0	39,035	39,035	3.1
VNPaaS	1,211	31,703	32,915	3.1

Table 8. Summary comparison of deployment models across decision KPIs

KPI	Legacy	Owned vEPC	NFVIaaS	VNPaaS	VNSaaS
OpEx reduction	L	VH	M	M	L
QoS/SLA assurance	M	VH	H	M	M
Regulatory mitigation	L	H	M	M	L–M
Operational complexity	L	H	H	M	M
Security control	H	H	M	M	L–M
Time to market	M	VH	H	M	M
Value proposition	L	H	M	H	H
CapEx reduction	L	M	H	VH	VH
Management complexity	L	M	M	H	H
Implementation complexity	L	M	M–H	H	H
Regulatory compliance	M	H	M	M	L–M
Overall case fit	L	VH	H	M	M

VH: very high, H: high, M: medium, and L: low. Ratings denote relative suitability under the same case scenario

4.3. Scenario-based technical validation

Because the ranking includes performance-related claims, the results are complemented by scenario-based technical validation under normal-load, peak-load, and stress-load conditions as shown in Table 9. End-to-end delay is decomposed as (8).

$$L_{\text{e2e}} = L_{\text{proc}} + L_{\text{queue}} + L_{\text{trans}} + L_{\text{ctrl}}, \tag{8}$$

where the terms represent processing, queuing, transport, and control/orchestration delay. Scalability is interpreted through an elasticity indicator:

$$E_m = \frac{\Delta C_m}{\Delta T_m + \Delta O_m}, \tag{9}$$

where ΔC_m is additional capacity, ΔT_m is time to activate capacity, and ΔO_m is additional operational effort or dependency. Owned vEPC can reduce queuing pressure through local VNF scaling while preserving direct function-placement, monitoring, and lifecycle control. NFVIaaS also offers elasticity, but provider dependence may affect transport delay, SLA enforcement, and root-cause visibility.

This validation does not claim live-network measurement; rather, it provides an analytical performance basis for the case-study ranking. It supports the conclusion that owned vEPC is preferred not only because of financial scoring but also because it provides the most coherent balance of latency governance, elastic scaling, recovery control, and observability. A live pilot remains necessary before commercial rollout.

Table 9. Condensed technical validation matrix

Dimension	Legacy	Owned vEPC	NFVIaaS	VNPaaS	VNSaaS
Latency/QoS	Stable but rigid	Best local control	Good, provider affected	Platform constrained	SLA/service dependent
Peak-load scaling	Hardware-bound	High elasticity	High but external	Medium	Medium
Recovery	Slow appliance recovery	VNF migration/local orchestration	Provider-dependent	Platform-dependent	Service-dependent
Observability	Vendor-specific	Full local visibility	Interface-limited	Abstracted	Most abstracted
Utilization	Low pooling	High pooling/control	High pooling	Medium–high	Provider-managed

4.4. Robustness interpretation and sensitivity analysis

A qualitative sensitivity analysis was added to test whether the conclusion depends excessively on a single KPI group. Three interpretation scenarios were examined. The first is the base case, where technical deployment has the highest influence because the operator must preserve service control and continuity. The second is a cost-constrained case, where CapEx pressure is stronger and outsourced models are expected to benefit. The third is a governance-constrained case, where security, regulatory exposure, observability, and troubleshooting control dominate. Table 10 summarizes the expected ranking stability.

The sensitivity interpretation shows that the owned vEPC recommendation is robust when the decision emphasizes long-term control, service quality, security, regulatory accountability, and OpEx optimization. However, the ranking is not universal. If a different operator has very limited capital, strong trust in an NFVI provider, mature cloud regulation, and less strict control requirements, NFVIaaS or VNPaaS may become more competitive. This reinforces the main purpose of the proposed framework: it is not a fixed ranking tool, but a transparent decision process that can be recalibrated for other operators and markets.

Table 10. Sensitivity interpretation of the deployment-model ranking

Scenario	Expected strongest model	Interpretation
Base-case weighting	Owned NFV/vEPC	Balanced control, OpEx reduction, QoS governance, and technical fit keep owned vEPC first
CapEx-emphasis scenario	NFVIaaS or VNPaaS	Outsourced or platform-based models improve when initial investment dominates the decision
Governance-emphasis scenario	Owned NFV/vEPC	Local control, observability, compliance, and security accountability strengthen owned vEPC
Rapid-service scenario	VNPaaS or VNSaaS	Service-based models improve when fast service consumption is prioritized over deep core control
Stress-load scenario	Owned NFV/vEPC or NFVIaaS	Elastic scaling is important; owned vEPC retains stronger visibility and recovery control

4.5. General discussion

The ranking should be interpreted in the economics of constrained mobile markets, where OpEx control, QoS continuity, local accountability, and regulatory risk are central to architecture choice. The framework's practical value is that it makes explicit why a low-CapEx outsourced model may be less suitable when data control, security responsibility, troubleshooting autonomy, supply-chain exposure, and long-term governance are important. It therefore differs from studies that report resource-allocation, slicing, or testbed performance gains after a core architecture has already been selected.

The result also shows that cost should not be interpreted only through initial capital expenditure. VNSaaS and VNPaaS reduce upfront ownership cost, but their recurring service fees, SLA premiums, and provider-dependent operations increase long-term exposure. NFVIaaS offers a stronger balance for capital-constrained operators, but it still transfers infrastructure visibility and some recovery responsibilities to the provider. Owned NFV/vEPC is less attractive when only short-term CapEx is considered, yet it becomes the strongest option when service control, observability, recovery, security accountability, and OpEx optimization are included.

For the Palestinian case, regulatory uncertainty and infrastructure restrictions increase the value of local control. The preferred model should therefore support technical modernization without creating unnecessary dependence on external platforms or opaque SLA enforcement. This explains why owned vEPC emerges as the strongest case fit, while outsourced service models remain useful as partial, transitional, or hybrid options rather than as full replacements for operator-controlled core governance.

4.6. Practical implications for emerging-market operators

The proposed framework has several practical implications beyond the Wataniya Mobile case. First, it provides a structured way to separate short-term affordability from long-term suitability. Operators often compare deployment models primarily through procurement cost, but this may conceal recurring service charges, escalation delay, platform dependency, and loss of observability. The TCO and technical-validation layers help reveal these hidden dimensions.

Second, the framework highlights that the migration path can be phased. A constrained operator does not need to move directly from legacy EPC to a full cloud-native core. A practical roadmap may begin with a limited vEPC proof of concept, continue with partial virtualization of selected EPC functions, and then expand toward broader NFV/MANO integration after staff skills, operational processes, monitoring tools, and security controls mature. This phased interpretation reduces implementation risk while preserving the long-term target architecture.

Third, the model can support executive communication. Technical teams usually evaluate scalability, redundancy, recovery, and observability, while business teams focus on CapEx, OpEx, vendor contracts, and time to market. Regulatory and security teams focus on data control, compliance, and accountability. By placing these concerns in one matrix, the framework allows decision makers to see how the selected model performs across multiple organizational viewpoints rather than treating the choice as a purely technical or purely financial decision.

Fourth, the framework can be used as a migration-control instrument. The operator can define decision gates before each implementation phase. At each gate, the team can reassess technical readiness, cost exposure, vendor dependency, regulatory constraints, security posture, and measurable service quality. This is especially important in emerging markets because procurement delays, infrastructure restrictions, and cloud-readiness gaps may change the feasibility of the selected model during implementation. Table 11 provides a compact roadmap that keeps the paper practical while avoiding unsupported claims of a completed pilot deployment.

Table 11. Suggested phased roadmap for applying the selected vEPC model

Phase	Main activity	Decision gate
Readiness audit	Review EPC assets, skill gaps, monitoring tools, and regulatory constraints	Confirm that virtualization scope and risk boundaries are clear
Proof of concept	Deploy limited vEPC functions in a controlled lab or isolated environment	Validate functionality, orchestration behavior, and operational visibility
Controlled field trial	Test selected functions under limited live-traffic conditions	Measure latency, availability, recovery, and troubleshooting performance
Gradual migration	Expand virtualization to additional functions or traffic domains	Confirm that SLA, security, and operational processes remain stable
Optimization	Tune scaling policies, resource allocation, cost controls, and monitoring	Recalibrate KPI weights and update the model ranking if conditions change

This roadmap is also useful for preventing overgeneralization. The conclusion that owned vEPC is preferred in this study should be treated as a case-specific decision result supported by cost modelling, expert judgment, robustness interpretation, and scenario-based validation. It should not be read as a universal claim that all emerging-market operators must adopt the same model. The framework remains transferable, but the weights, cost values, provider assumptions, and regulatory inputs must be recalibrated for each operator shown in Table 12.

Table 12. Practical use of the framework by operator stakeholders

Stakeholder group	How the framework supports the decision
Network engineering	Compares scalability, latency exposure, redundancy, and function-placement control
Operations and QoS teams	Evaluates observability, troubleshooting visibility, SLA assurance, and recovery behavior
Security and regulatory teams	Examines data control, provider dependency, compliance exposure, and accountability boundaries
Finance and procurement	Compares CapEx, recurring OpEx, TCO, SLA premiums, and long-term vendor dependency
Executive management	Links the technical architecture decision to strategic control, investment risk, and service differentiation

4.7. Limitations

The study remains a case-study-based decision analysis and should not be interpreted as a universal ranking of EPC deployment models. The results depend on the Palestinian operator context, the selected KPI set, the expert-panel judgments, and the five-year TCO assumptions. In markets with mature cloud regulation, stronger national NFVI providers, lower connectivity risk, or different traffic profiles, NFVIaaS or platform-based models may receive stronger rankings. In addition, the technical validation is scenario-based and analytical; it supports the interpretation of the ranking but does not replace live measurements. These limitations are addressed by the future pilot-validation path proposed below.

4.8. Future work

Future work should validate the ranking through staged pilot deployments, beginning with a limited vEPC proof of concept and controlled field trials. Measured indicators should include latency, jitter, packet loss, throughput, availability, VNF instantiation time, scaling time, recovery time, troubleshooting duration, resource utilization, and energy consumption [12], [14], [15]. The measured values can then be compared with the predicted KPI scores to recalibrate the weighting and scoring matrix.

A second extension is to model edge-enabled EPC and 5G-core placement. Future versions should evaluate the placement of control-plane and user-plane functions across central cloud, regional cloud, and edge sites. This would allow the framework to account for local breakout, transport cost, edge-site availability, orchestration overhead, energy footprint, and UPF/vUPF placement decisions [16], [28].

A third extension is multi-operator slicing and infrastructure sharing. In emerging markets, shared NFVI, neutral-host deployments, and cross-operator slice federation may become attractive because of spectrum scarcity, capital limitations, and infrastructure restrictions. Extending the framework in this direction requires additional KPIs for slice isolation, inter-operator governance, data ownership, cross-domain SLA assurance, regulatory compliance, and revenue-sharing mechanisms [13], [17], [18].

5. CONCLUSION

This paper presented a compact, context-aware decision framework for selecting EPC virtualization strategies in an emerging Palestinian mobile-network scenario. The framework combines expert-based KPI elicitation, AHP-supported weighting, weighted scoring, TOPSIS-style robustness checking, five-year TCO estimation, and scenario-based technical validation. The analysis indicates that owned NFV/vEPC provides the strongest overall fit for Wataniya Mobile when OpEx reduction, QoS/SLA assurance, operational control, security governance, regulatory exposure, implementation constraints, and long-term service flexibility are considered together. NFVIaaS and VNPaaS remain useful alternatives for operators prioritizing lower initial CapEx, but their provider-dependency and governance limitations reduce their overall suitability in this case. The proposed framework can support similar deployment-selection decisions in other constrained emerging markets, provided that KPI weights and cost assumptions are recalibrated to the local regulatory, traffic, cloud-readiness, and business environment.

ACKNOWLEDGMENTS

The authors thank all Wataniya Mobile participants who contributed through interviews and technical discussions. This research was not supported by any external research grant or contract. The article processing and publication charges were self-funded by the authors.

FUNDING INFORMATION

Authors state no funding involved. The work and publication charges were self-funded by the authors.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Saed Tarapiah	✓	✓		✓	✓	✓			✓	✓	✓	✓	✓	
Shadi Atalla		✓		✓	✓					✓		✓		
Khawla Hafiz Daraghme					✓	✓	✓	✓		✓				

C	: **C**onceptualization	I	: **I**nvestigation	Vi	: **Vi**sualization
M	: **M**ethodology	R	: **R**esources	Su	: **Su**pervision
So	: **So**ftware	D	: **D**ata Curation	P	: **P**roject Administration
Va	: **Va**lidation	O	: Writing - **O**riginal Draft	Fu	: **Fu**nding Acquisition
Fo	: **Fo**rmal Analysis	E	: Writing - Review & **E**diting		

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

The study used anonymized expert and stakeholder input. No personal identifying data are disclosed. Informed consent was obtained from the individuals involved in the discussions.

ETHICAL APPROVAL

The study did not involve medical intervention, animal subjects, or personally identifiable human-subject data. The expert input was anonymized and used for technical and managerial decision analysis.

DATA AVAILABILITY

Derived data supporting the findings of this study are available from the corresponding author upon reasonable request, subject to confidentiality and operator-related restrictions.

REFERENCES

[1] GSMA Intelligence, “*The Mobile Economy 2017*,” London, U.K.: GSM Association, 2017.
[2] GSMA Intelligence, “*The Mobile Economy: Middle East and North Africa 2017*,” London, U.K.: GSM Association, 2017.
[3] COMCEC, “*Increasing Broadband Internet Penetration In the OIC Member Countries*,” Ankara, COMCEC, 2016.
[4] GSMA Intelligence, “*Understanding 5G: Perspectives on future technological advancements in mobile*,” London, U.K.: GSM Association, 2014.
[5] ETSI, “*Network Functions Virtualisation (NFV); Architectural Framework*,” GS NFV 002 V1.2.1, 2013.
[6] K. Park, S. Sung, H. Kim, and J. Jung, “Technology trends and challenges in SDN and service assurance for end-to-end network slicing,” *Computer Networks*, vol. 234, p. 109908, Oct. 2023, doi: 10.1016/j.comnet.2023.109908.
[7] R. Patil, Z. Tian, M. Gurusamy, and J. McCloud, “5G core network control plane: Network security challenges and solution requirements,” *Computer Communications*, vol. 229, 2025, doi: 10.1016/j.comcom.2024.107982.
[8] R. W. Coêlho, R. A. Silva, L. A. F. Martimiano, and E. J. Leonardo, “IoT and 5G Networks: A Discussion of SDN, NFV and Information Security,” *Journal of the Brazilian Computer Society*, vol. 30, no. 1, pp. 212–227, 2024, doi: 10.5753/jbcs.2024.3021.
[9] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, “Network Function Virtualization: State-of-the-Art and Research Challenges,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 236–262, 2016, doi: 10.1109/comst.2015.2477041.
[10] Credence Research, “*Network Function Virtualization (NFV) Market Size and Forecast to 2032*,” 2024.
[11] J. Wu, Y. Gao, L. Wang, J. Zhang, and D. O. Wu, “How to Allocate Resources in Cloud-Native Networks Towards 6G,” *IEEE Network*, vol. 38, no. 2, pp. 240–246, 2024, doi: 10.1109/MNET002.2300017.
[12] M. Zieba, M. Natkaniec, and P. Borylo, “Cloud-Enabled Deployment of 5G Core Network with Analytics Features,” *Applied Sciences (Switzerland)*, vol. 14, no. 16, 2024, doi: 10.3390/app14167018.
[13] M. Dalgitsis, N. Cadenelli, M. A. Serrano, N. Bartzoudis, L. Alonso, and A. Antonopoulos, “Cloud-Native Orchestration Framework for Network Slice Federation Across Administrative Domains in 5G/6G Mobile Networks,” *IEEE Transactions on Vehicular Technology*, vol. 73, no. 7, pp. 9306–9319, 2024, doi: 10.1109/TVT.2024.3362583.
[14] C. E. Menin *et al.*, “Enabling Cloud-Native Observability for White-Box Performance Analysis of the 5G Core,” *in Proceedings of IEEE/IFIP Network Operations and Management Symposium 2025, NOMS 2025*, IEEE, May 2025, pp. 1–6, doi: 10.1109/NOMS57970.2025.11073613.
[15] A. Bellin, N. Di Cicco, D. Munaretto, and F. Granelli, “Energy and performance analysis of virtualized 5G core network on distributed edge nodes,” *Computer Networks*, vol. 249, 2024, doi: 10.1016/j.comnet.2024.110538.
[16] A. Bellin, N. Di Cicco, D. Munaretto, and F. Granelli, “Power Consumption-Aware 5G Edge UPF Selection using Deep Reinforcement Learning,” *2024 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). IEEE*, pp. 1–6, Nov. 05, 2024. doi: 10.1109/nfv-sdn61811.2024.10807472.
[17] V.-G. Nguyen, A. Brunstrom, K.-J. Grinnemo, and J. Taheri, “SDN/NFV-Based Mobile Packet Core Network Architectures: A Survey,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1567-1602, 2017, doi: 10.1109/COMST.2017.2690823.
[18] Z. Allaw, O. Zein, and A.-M. Ahmad, “Cross-Layer Security for 5G/6G Network Slices: An SDN, NFV, and AI-Based Hybrid Framework,” *Sensors*, vol. 25, no. 11, p. 3335, May 2025, doi: 10.3390/s25113335.
[19] A. Simha, *NFV Reference Architecture for Deployment of Mobile Networks*, Version 1.0. Red Hat, Dec. 2016.
[20] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, “Network function virtualization: Challenges and opportunities for innovations,” *IEEE Communications Magazine*, vol. 53, no. 2, pp. 90-97, Feb. 2015, doi: 10.1109/MCOM.2015.7045396.
[21] T. L. Saaty, *The Analytic Hierarchy Process : Planning , Priority Setting , Resource Allocation*,. New York, NY, USA: McGraw-Hill, 1980.
[22] R. W. Saaty, “The analytic hierarchy process—what it is and how it is used,” *Mathematical Modelling*, vol. 9, no. 3–5, pp. 161–176, 1987, doi: 10.1016/0270-0255(87)90473-8.
[23] C.-L. Hwang and K. Yoon, *Multiple Attribute Decision Making: Methods and Applications A State-of-the-Art Survey*. Berlin: Springer, 1981.
[24] A. G. Papidas, “*Network Functions Virtualization (NFV) for Mobile Networks*,” Athens University of Economics and Business, 2016.
[25] D. Boniecki, C. Marcati, W. Abou-Zahr, T. Alatovic, and O. El Hamamsy, *Middle East and Africa Telecommunications Industry at Cliff's Edge: Time for Bold Decisions*. McKinsey & Company, 2016.
[26] F. Antão, H. R. Chi, D. Corujo, V. A. Cunha, M. Sanchez, and R. L. Aguiar, “Toward Decarbonized Network Function Virtualization-

Based ICT Management: Standardization, Architecture, and Challenges," *IEEE Communications Standards Magazine*, vol. 10, no. 1, pp. 162–170, Mar. 2026, doi: 10.1109/MCOMSTD.2025.3595284.

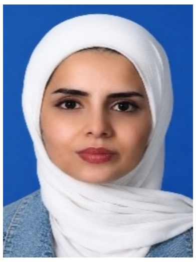
[27] M. Vutukuru, N. Sadagopan, P. Satapathy, and J. K. Dave, "A virtualized evolved packet core for LTE networks," *Indian Institute of Technology Bombay, Mumbai, India*, 2016. [Online]. Available: https://github.com/networkedsystemsIITB/NFV_LTE_EPC

[28] L. Wernet, L.-M. Spang, F. Siegmund, and T. Meuser, "Resilient User Plane Traffic Redirection in Cellular Networks," in *2024 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), IEEE*, Nov. 2024, pp. 1–6, doi: 10.1109/NFV-SDN61811.2024.10807476.

BIOGRAPHIES OF AUTHORS

Saed Tarapiah is an Associate Professor in the Department of Telecommunication Engineering at An–Najah National University in Nablus, Palestine. He holds a Ph.D. in Electronics and Telecommunications Engineering and a Master's degree in Information Technology from Politecnico di Torino, Italy, earned summa cum laude. His research focuses on wireless sensor networks, IoT, vehicular communications, and real-time healthcare monitoring systems. He has published extensively on network performance, smart agriculture, indoor localization, and low-cost home automation. He is committed to applying advanced telecommunications technologies to practical challenges in health, transportation, and sustainability. He can be contacted at email: s.tarapiah@najah.edu.

Shadi Atalla is a faculty member at the College of Engineering and Information Technology, University of Dubai, United Arab Emirates. With a strong academic background and extensive experience in engineering and information technology, he has contributed to teaching and research in telecommunications, signal processing, and emerging technologies in smart systems. He is involved in curriculum development and academic innovation and has published in reputable journals and participated in international conferences. He can be contacted at email: satalla@ud.ac.ae.



Khawla Hafiz Daraghme is a Senior Demand and Technology Projects Engineer with extensive experience in the telecommunications sector. She specializes in aligning business requirements with technology solutions, leading complex technology projects, and supporting strategic planning and budgeting initiatives. She holds a strong academic background in engineering management and telecommunications engineering, with expertise in demand management, business analysis, governance and risk management, and evaluation of emerging market and technology trends. Her professional work contributes to technology planning, demand governance, and strategic telecom transformation in operational environments. She can be contacted at email: Khawladara@gmail.com.