DOI: https://doi.org/10.36910/6775-2524-0560-2026-62-05
UDC 004.056.5:004.7:621.391
Bobyk Yurii, PhD student
https://orcid.org/0009-0001-5717-8745
National University «Lviv Polytechnic», Lviv, Ukraine

AN INTEGRATED QOS/QOE EVALUATION METHOD FOR INFORMATION SERVICES IN DISTRIBUTED NETWORKS

Bobyk Y. An integrated QoS/QoE evaluation method for information services in distributed networks. The escalating complexity of distributed networks, combined with persistent exposure to adversarial traffic and automated security enforcement, has rendered traditional, siloed approaches to service quality evaluation increasingly inadequate. In such environments, security decisions no longer operate as neutral protective measures; instead, they actively reshape network behavior and, by extension, the perceived quality of information services. This paper addresses the problem of fragmented assessment of Quality of Service (QoS) and Quality of Experience (QoE) by proposing an integrated evaluation method explicitly embedded within an adaptive security loop. The proposed approach introduces a mathematically grounded framework in which attack detection, mitigation intensity, and service-level performance are treated as interdependent components of a single dynamic system. QoS indicators derived from aggregated traffic observations are transformed into a normalized QoE proxy and further fused with security overhead through a unified utility function. This formulation enables continuous, real-time quantification of how security actions – such as DDoS mitigation, access control enforcement, and cryptographic protection – affect both technical service characteristics and user-perceived continuity. To validate the feasibility of the model, a modular software prototype was developed and evaluated using a publicly available labeled network traffic dataset containing benign and DDoS attack scenarios. Experimental results demonstrate that the proposed quality-aware adaptive strategy preserves user experience more consistently than a baseline security-centric approach while maintaining equivalent attack detection capability. The findings confirm that embedding QoS/QoE evaluation directly into the security control loop enables more balanced and resilient decision-making, positioning the proposed method as a viable foundation for quality-aware security management in modern distributed information services.
Keywords: Quality of Service; Quality of Experience; adaptive security loop; distributed networks; DDoS mitigation; utility-based evaluation; machine learning-driven intrusion detection; service quality assessment; quality-aware network control

Бобик Ю.В. Інтегрований метод оцінки QoS/QoE для інформаційних послуг у розподілених мережах. Зростаюча складність розподілених мереж у поєднанні з постійним впливом ворожого трафіку та автоматизованим забезпеченням безпеки робить традиційні ізольовані підходи до оцінювання якості сервісів дедалі менш ефективними. У таких середовищах рішення у сфері безпеки вже не виступають нейтральними захисними механізмами, а активно змінюють поведінку мережі та, відповідно, сприйману якість інформаційних сервісів. У статті розв'язується проблема фрагментарного оцінювання якості обслуговування (QoS) та якості досвіду користувача (QoE) шляхом запропонування інтегрованого методу оцінювання, безпосередньо вбудованого в адаптивний контур безпеки. Запропонований підхід ґрунтується на математично формалізованій моделі, у якій виявлення атак, інтенсивність протидії та продуктивність сервісу розглядаються як взаємопов'язані компоненти єдиної динамічної системи. Показники QoS, отримані на основі агрегованих спостережень трафіку, трансформуються у нормалізований проксі-показник QoE та поєднуються з накладними витратами безпеки в межах єдиної функції корисності. Така постановка забезпечує безперервну оцінку в реальному часі впливу заходів безпеки — зокрема протидії DDoS-атакам, механізмів контролю доступу та криптографічного захисту — на технічні характеристики сервісу та сприйману користувачем безперервність обслуговування. Для перевірки працездатності моделі розроблено модульний програмний прототип, який апробовано на відкритому маркованому наборі мережевого трафіку, що містить сценарії нормальної роботи та DDoS-атак. Експериментальні результати демонструють, що запропонована адаптивна стратегія, орієнтована на якість, забезпечує більш стабільне збереження користувацького досвіду порівняно з базовим підходом, орієнтованим виключно на безпеку, при збереженні еквівалентної здатності до виявлення атак. Отримані результати підтверджують, що інтеграція оцінювання QoS/QoE безпосередньо в контур керування безпекою сприяє більш збалансованому та стійкому прийняттю рішень і може слугувати основою для управління безпекою з урахуванням якості в сучасних розподілених інформаційних сервісах.
Ключові слова: якість обслуговування; якість досвіду користувача; адаптивний контур безпеки; розподілені мережі; протидія DDoS-атакам; оцінювання на основі функції корисності; виявлення вторгнень на основі машинного навчання; оцінювання якості сервісу; керування мережею з урахуванням якості.

Statement of a scientific problem.

Contemporary distributed networks increasingly operate under conditions where service delivery, security enforcement, and user perception are inseparably intertwined. Information services deployed across cloud-edge-core continuums are continuously exposed to adversarial traffic, dynamic load variations, and heterogeneous control decisions, all of which directly affect both measurable Quality of Service parameters and the less tangible but no less critical Quality of Experience perceived by end users. Despite substantial progress in intrusion detection, adaptive security mechanisms, and QoS optimization techniques, the dominant body of research still treats service quality evaluation and security response as loosely coupled or sequential processes.

In existing approaches, Quality of Service is typically quantified through isolated network-centric metrics such as latency, throughput, or packet loss, while Quality of Experience is either approximated indirectly or confined to specific application domains. Security mechanisms, in turn, are often evaluated primarily by detection accuracy or attack mitigation efficiency, with limited consideration of how defensive actions themselves reshape service behavior and user perception. This fragmentation results in a methodological gap: security decisions may be technically correct yet operationally harmful, as excessive or poorly calibrated mitigation can degrade service continuity, responsiveness, and overall utility without yielding proportional security benefits.

The scientific problem addressed in this study therefore lies in the absence of a unified, quantitatively grounded framework that enables joint evaluation of QoS and QoE within an adaptive security loop of distributed networks. Specifically, there is no widely accepted method that can continuously translate security decisions into measurable service-quality consequences, reconcile network-level performance indicators with experience-oriented proxies in a comparable manner across heterogeneous information services, and support real-time decision-making under partial observability and adversarial dynamics. The lack of such an integrated evaluation paradigm hinders principled trade-off analysis between protection strength and service preservation, ultimately limiting the effectiveness and sustainability of security-aware network management.

Research analysis. The recent body of work on distributed networks increasingly treats service quality as a multi-layer phenomenon, where network-level QoS guarantees must be interpreted through user-perceived QoE and validated under realistic multi-domain constraints.

Sha and co-authors propose a QoE-aware edge server placement model for mobile edge computing, formulating the problem as an optimization task that explicitly couples placement decisions with QoE outcomes, and then solving it via an enhanced genetic algorithm that incorporates adaptive crossover and an elite-retention strategy to stabilize convergence [1]. Methodologically, the work combines a QoE-oriented objective design for edge placement with metaheuristic search and benchmarking against both an exact (small-scale) solver and representative heuristics. The measured results are reported as high-quality placement solutions with QoE reaching about 78%, remaining within ~3% of the optimal in small instances, achieving roughly 42% improvement in solution efficiency compared to compared methods, and doing so with practical runtime on the order of a few seconds [1]. The significance of this contribution is that it makes QoE an optimization target rather than a post-hoc observation; however, what remains unresolved is how such QoE-centric placement outputs should be translated into a unified evaluation layer that is comparable across heterogeneous services (e.g., telemetry, control-plane services, media delivery) and across domains with distinct observability. This gap is partly objective – QoE is inherently service- and context-dependent and cannot be reduced to a single universal metric without losing meaning – and partly methodological, since most placement studies validate gains in a controlled simulation setting rather than in a broader end-to-end monitoring pipeline that also accounts for policy, security overhead, and cross-domain measurement bias.

Marwan and collaborators examine cloud-edge data centers through a joint lens of security, QoS, and energy, modeling the interaction between participants using game theory and incorporating homomorphic encryption to protect sensitive data flows while still enabling optimization [2]. Their approach couples formal modeling (game-theoretic formulation) with cryptographic design choices and a verification mindset (formal verification) to ensure that the optimized strategies remain valid under the assumed adversarial and operational constraints. The measurable results include comparative cryptographic performance observations, such as a reported throughput advantage of Paillier over RSA by more than a factor of two in their evaluated setting, alongside evidence that the optimization can be executed while preserving confidentiality properties [2]. The key value for an integrated evaluation agenda lies in the fact that security mechanisms are treated as first-class constraints that shape QoS and energy behavior rather than as external add-ons. Yet, a major unresolved issue is the lack of a standardized way to quantify how cryptographic protection and verification guarantees should be "priced" into user-perceived quality: encryption overhead and verification constraints affect latency and availability, but the mapping to QoE is not explicitly formalized. This remains unresolved largely for objective reasons (cryptographic overhead is workload- and deployment-dependent, and verification models require assumptions that rarely hold uniformly in operational networks) and subjective reasons (research often prioritizes demonstrating feasibility of secure optimization rather than building a harmonized, service-agnostic evaluation layer that can be reused across scenarios).

Dhandapani with co-workers address QoS-aware routing for network slicing in multi-domain SDN by introducing a cooperative multi-agent DRL framework that combines hierarchical SDN control, a distributed global topology procedure for inter-domain path reasoning, and an MPNN-based TD3 learning strategy for selecting end-to-end routes under delay and bandwidth requirements [3]. The evaluation emphasizes operational QoS indicators at scale: they report throughput gains such as 603 Mbps at 1000 path requests versus 502 Mbps for a baseline DeepRMSA scheme, and show that other compared routing systems fall markedly behind as load increases (e.g., SAP about 67.6% lower throughput at 5000 requests), while packet loss is consistently lower than alternatives (with other baselines exhibiting ~37.5-42.0% packet loss at 1000 requests in the cited comparison) [3]. They further quantify scalability via rejection-rate reductions, showing sizeable advantages of CoopAI-Route over heuristics under both moderate and heavy load and providing millisecond-level online processing times for inter-domain requests [3]. The significance here is that the work demonstrates how QoS enforcement can be learned and sustained under multi-domain uncertainty – exactly the sort of environment where end-user quality is often degraded by cross-domain congestion and inconsistent policy. However, what remains unresolved is how such DRL-driven QoS compliance should be integrated into a broader QoS/QoE evaluation framework that is explainable, auditable, and consistent across operators; DRL policies can optimize measurable QoS but still fail to provide transparent QoE accountability. This persists for objective reasons (multi-domain operators cannot freely share state and labels, restricting consistent measurement and training) and subjective reasons (evaluation traditions in DRL networking focus on comparative performance curves rather than on cross-service interpretability and unified measurement design).

Barakabitze and a co-author provide a survey and conceptual ecosystem for QoE-driven multimedia delivery using SDN/NFV in 5G/6G directions, emphasizing that QoE management has historically been less addressed than raw performance provisioning and proposing a generalized QoE provisioning ecosystem alongside technology roadmaps and ML-based controller perspectives [4]. The measurable outcome in a survey context is the structured synthesis: defined use-case classes (QoE-driven management across cloud/edge, QoE monitoring under traffic variation, ML-based QoE provisioning) and an articulated set of challenges and research directions for orchestration and monitoring of future immersive multimedia services [4]. The relevance to integrated evaluation is that the paper clarifies that QoE must be operationalized through monitoring and orchestration loops – not merely inferred – yet it also exposes an unresolved problem: QoE frameworks in surveys often remain domain-specific (multimedia-centric) and do not fully generalize to broader information services like distributed telemetry, control, or security monitoring. The objective reason is that QoE features are service-type dependent and heavily influenced by user context; the subjective reason is that the community has fragmented into vertical application silos, each developing its own QoE proxies, making unification difficult.

Shaji together with a colleague survey security aspects of distributed SDN controllers in enterprise SD-WLAN, focusing on the tension between logical centralization and physical distribution for scalability and resilience, while emphasizing security, consistency, reliability, and controller placement issues [5]. Their "measured" contribution is the consolidated set of security issues and proposed solution directions (e.g., identity frameworks, traceability, controller placement policies, and controller-network hardening measures) grounded in the SD-WLAN enterprise setting [5]. This is important because distributed control planes are foundational to distributed information services and their QoS behavior; controller compromise or inconsistency can degrade availability and induce QoE failures indirectly. The unresolved issue is that security hardening recommendations are rarely tied to quantified service-quality impacts: it remains unclear how to incorporate controller security posture, synchronization overhead, and failover behavior into a unified QoS/QoE evaluation. Objectively, controlled experiments are difficult because enterprise SD-WLAN deployments differ widely; subjectively, security surveys often stop at qualitative prescriptions rather than proposing measurable, cross-layer evaluation schemas.

Qazi and colleagues present a taxonomy-focused survey of SLA techniques in cloud computing, framing SLAs as the contractual layer that formalizes SLOs tied to QoS and discussing evaluation parameters, analysis platforms, design objectives, and open research issues [6]. The measurable result here is the taxonomy itself and the structured identification of evaluation parameters and open issues that impede robust SLA provisioning and management [6]. For an integrated evaluation perspective, the key insight is that QoS/QoE evaluation cannot be separated from what is contractually guaranteed and monitored; however, an unresolved gap remains in bridging SLA/SLO constructs with end-user QoE: most SLA frameworks still treat QoE as indirect or absent, and multi-domain distributed services complicate

accountability (who "owns" a QoE violation when a service spans edge, core, and third-party components?). The objective reason is legal and operational heterogeneity across providers; the subjective reason is that many SLA studies prioritize formal taxonomies and negotiation mechanisms rather than operational measurement pipelines that unify QoS and QoE.

Ergen and co-authors provide a comprehensive evaluation and vision for edge computing in future wireless networks toward 6G, emphasizing heterogeneous resource coordination, near-real-time resource utilization (links, storage, computation), and the need for networks to incorporate resource availability and reputational information to ensure QoE [7]. Their measurable contribution is the systematic coverage of architectural frameworks and the identification of research gaps across resource allocation, computation delegation, data administration, and network management, including emphasis on sustainability and standards [7]. This is crucial because integrated QoS/QoE evaluation requires a stable conceptual map of where and how quality is affected across the edge continuum. Yet, a persistent unresolved question is how to operationalize unified QoS/QoE evaluation in partially observed and reputation-influenced systems: quality becomes a moving target when orchestration decisions adapt in near real-time and when trust/reputation signals affect routing or placement. Objectively, 6G architectures and standards are still evolving, limiting real testbeds; subjectively, the literature often catalogs gaps without converging on shared measurement primitives for integrated evaluation.

Ibrahim AlShathri with co-authors study SDN-based fog architectures under overload conditions, proposing a dynamic "second offloading" service that decides whether tasks should be offloaded again (fog-to-fog or fog-to-cloud) based on task type, latency constraints, resource needs, and priority heuristics coordinated via an SDN controller [8]. The measured results include an improvement of about 33% in the average time required to select offloading nodes compared to a dynamic fog-to-fog offloading baseline, as well as improved workload distribution behavior for certain classes of tasks [8]. This work matters because it connects service quality degradation (overload, latency constraints) to an explicit control decision and provides quantifiable benefits. The unresolved issue is that offloading decisions are usually evaluated with network-centric QoS metrics (selection time, latency adherence) rather than with a consistent mapping to QoE across service types. Objectively, QoE ground truth is harder to define for generic IoT/fog workloads than for human-facing media; subjectively, evaluation is frequently constrained to simulation KPIs that are easiest to measure.

Wu and collaborators address optimal deployment of IoT services on fog computing via a metaheuristic-based multi-objective approach, emphasizing that deployment decisions should balance multiple competing objectives and reporting a structured comparison of existing studies, their performance metrics (latency, cost, response/service time, resource utilization, energy, throughput, deadlines), achievements, and weaknesses [9]. Their measurable output is the systematic multi-metric lens and the explicit identification of recurring weaknesses – e.g., many prior solutions omit reliability/availability or fail to model trade-offs between different QoS dimensions – thereby motivating multi-objective optimization as an architectural necessity [9]. The unresolved problem is that, even when multi-objective QoS optimization is performed, it rarely yields a unified evaluation method that integrates user experience signals or cross-domain measurement consistency. This persists objectively because multi-objective outputs are inherently Pareto-based and difficult to collapse into a single operational score, and subjectively because research communities often treat "multi-objective optimization achieved" as an endpoint rather than designing standardized evaluation interfaces that connect results to QoE.

Ostrowski and co-authors survey mobility-aware fog computing with mobile nodes, highlighting that dynamic topologies and time-varying characteristics of both fog nodes and users make mobility-awareness challenging and systematically underexplored; they review models grounded in opportunistic networking, social communities, temporal networks, and vehicular ad-hoc networks, and critically extract open issues and future directions [10]. The measurable contribution is again the consolidation of models and the explicit articulation of open problems tied to latency, energy, contextual information loss, intermittent connectivity, scalability, privacy, and security [10]. This is highly relevant because any integrated QoS/QoE evaluation in distributed networks must remain valid under mobility and partial observability. The unresolved issue is that mobility introduces non-stationarity: the same QoS metric threshold may correspond to different QoE perceptions depending on user movement and context, making stable evaluation difficult. Objectively, reproducing mobility patterns at scale is hard; subjectively, many works focus on proposing mobility-aware mechanisms without agreeing on shared evaluation baselines that unify QoS and QoE under mobility.

Tung and colleagues discuss AI-assisted continuous security monitoring over Open RAN SMO, treating monitoring as a "live" process integrated into orchestration and control planes and emphasizing automation and scalability of event collection and analysis pipelines without eroding service performance [11]. The measurable result is primarily architectural and operational: the feasibility of maintaining continuous observation and policy controllability in a multi-component environment, with evaluation typically framed through stability and scalability of monitoring/response under growth in events and functions [11]. The significance is that it reframes security monitoring as an operational service whose quality must be evaluated like any other network service, which pushes naturally toward integrated QoS/QoE thinking. The unresolved question is how to formalize and harmonize cross-domain policy coordination (RAN/edge/core) and confidentiality of monitoring data while scaling telemetry volumes – an issue that is objectively intensified by multi-vendor trust models and heterogeneous interfaces, and subjectively by the lack of commonly accepted metrics that bridge security effectiveness and user-perceived service continuity.

Hoque and co-authors review the resource consumption of ML in communications network security, proposing a taxonomy for reducing resource consumption across energy, computing, memory, latency, bandwidth, and human resources, and outlining challenges and future directions for resource-efficient ML-based security solutions [12]. Their measurable output is the resource-centric taxonomy and the explicit enumeration of the resource dimensions that constrain practical deployability and sustainability [12]. This is crucial for integrated QoS/QoE evaluation because ML-based monitoring and security increasingly sits in the critical path of distributed information services; resource overhead becomes a direct driver of latency and availability degradation, thereby shaping perceived quality. The unresolved issue is that, while resource dimensions are systematically categorized, there is still no widely adopted method that converts resource consumption and security automation benefits into an integrated quality evaluation that accounts for user impact. Objectively, workloads and deployments vary dramatically across networks; subjectively, the community often evaluates ML models by detection metrics and separate resource profiling, without integrating them into a single decision-theoretic evaluation framework.

Across the analyzed works, the unresolved questions converge on two tightly coupled gaps. First, despite clear advances in optimizing or enforcing QoS (routing, offloading, placement) and in conceptualizing QoE management (surveys and ecosystems), the literature does not yet provide a consistent, experimentally grounded methodology that integrates QoS and QoE into a unified evaluation layer suitable for heterogeneous information services spanning multiple domains and resource strata. Second, even when studies acknowledge cross-layer interactions – security vs performance, resource consumption vs latency, orchestration vs reliability – the mapping from low-level measurable KPIs (delay, throughput, loss, controller stability, compute/energy overhead) to user-relevant experience and service accountability remains fragmented and scenario-dependent. These questions remain unresolved for objective reasons: multi-domain systems restrict observability and information sharing; QoE is inherently contextual and service-specific; and realistic testbeds and representative datasets for end-to-end validation are limited or expensive. They also persist for subjective reasons: research is often organized in vertical silos (multimedia QoE, SDN security, fog offloading, DRL routing), and evaluation culture frequently favors domain-local benchmarks over shared measurement primitives and harmonized validation protocols.

Systematizing the local limitations reported in each source yields a single generalized unsolved problem: distributed networks lack a scalable, reproducible, and cross-domain evaluation method that jointly quantifies service-level QoS behavior and user-perceived QoE while explicitly accounting for orchestration decisions, security and ML overhead, and heterogeneous edge-cloud resource conditions, so that optimization outcomes (placement/routing/offloading/control) can be compared and governed consistently under realistic dynamics and partial observability. From this formulation, the research aim follows logically: to design and experimentally validate an integrated QoS/QoE evaluation method that defines a coherent set of measurable QoS primitives across layers, establishes a defensible mapping to QoE proxies tailored to information services, and supports multi-domain comparability by incorporating overhead, uncertainty, and accountability constraints into the evaluation logic rather than treating them as external factors.

Presentation of the main material and justification of the results of the study. The proposed mathematical model formalizes the evaluation of service quality in distributed networks as a tightly coupled interaction between traffic dynamics, adaptive security decisions, and service-level perception, rather than as a sequence of isolated monitoring and protection stages. In contrast to conventional formulations where

Quality of Service and Quality of Experience are assessed ex post, the model embeds QoS/QoE evaluation directly into the adaptive security loop, allowing security responses to be interpreted through their immediate and cumulative impact on information services.

Let the distributed network be represented as a set of observation nodes that continuously generate traffic flows, which are aggregated over discrete time windows to ensure scalability under high traffic intensity. For each time window t, the system state is captured by a feature vector

$$x_t = \left[x_t^{(1)}, x_t^{(2)}, \dots, x_t^{(n)}\right], \quad (1)$$

where the components describe aggregated traffic intensity, protocol composition, and structural diversity of sources and destinations. On the basis of x_t, a detection function estimates the instantaneous attack risk as a posterior probability

$$r_t = P(\text{attack} \mid x_t), \quad (2)$$

which serves as the driving signal for the adaptive security loop. Unlike static intrusion detection schemes, this risk estimate is not used solely for classification, but acts as a continuous control variable that modulates subsequent protection actions.

The adaptive security response is modeled as a pair of control parameters: a decision threshold θ_t governing attack mitigation and an intensity parameter $\mu_t \in [0,1]$ reflecting the strength of enforced countermeasures, including traffic filtering, access restriction, and cryptographic overhead. These parameters are allowed to vary over time, enabling the system to react proportionally to perceived risk rather than applying binary or fixed policies. As a result, the observable service behavior in window tis described by a vector of Quality of Service indicators

$$q_t = f(x_t, \mu_t), \quad (3)$$

where $f(\cdot)$ captures the transformation of raw traffic characteristics into measurable performance attributes such as effective throughput, delay proxies, and packet processing efficiency under the imposed security constraints.

Quality of Experience is introduced as a derived, service-oriented quantity that aggregates QoS indicators into a normalized proxy reflecting perceived continuity and responsiveness of information services. In the proposed model, QoE is expressed as a nonlinear mapping

$$QoE_t = g(q_t), \quad (4)$$

which intentionally avoids domain-specific subjective scales and instead relies on a monotonic transformation that preserves relative service degradation or improvement across time. This choice ensures that QoE remains comparable across heterogeneous information services while still being sensitive to performance disruptions induced by security actions.

The central element of scientific novelty lies in the formulation of an integrated utility functional that unifies QoS, QoE, and security overhead into a single evaluative criterion. For each time window, the system utility is defined as

$$U_t = \alpha\, QoS_t + \beta\, QoE_t - \gamma\, C(\mu_t), \quad (5)$$

where QoS_tdenotes an aggregate QoS score derived from q_t, $C(\mu_t)$quantifies the operational cost of security enforcement, and α, β, γ are weighting coefficients reflecting the relative importance of performance, user experience, and protection overhead. Unlike classical multi-objective formulations that optimize these dimensions independently, the proposed utility embeds them into a single, continuously evaluated functional, thereby enabling direct comparison of alternative security configurations under identical traffic conditions.

Within the adaptive loop, the decision-making process seeks parameter values (θ_t, μ_t)that maximize the expected utility over time,

$$(\theta_t^*, \mu_t^*) = \arg\max_{\theta,\mu} \; E[U_t \mid r_t], \quad (6)$$

effectively transforming security management into a quality-aware control problem. This perspective departs from traditional intrusion-centric reasoning by treating detection accuracy as a constraint rather than the ultimate objective, and by explicitly acknowledging that excessive protection may erode service value even when attacks are correctly identified.

The mathematical coherence of the model is reinforced by its window-based abstraction, which ensures that computational complexity scales with the number of observation intervals rather than raw packet volume. More importantly, the model establishes a bidirectional coupling between security and service evaluation: security decisions influence QoS and QoE through mitigation intensity, while QoS/QoE feedback implicitly shapes future security configurations via the utility maximization process. This

coupling represents a conceptual shift from static performance assessment toward a reflexive evaluation paradigm, where service quality and user experience are no longer passive indicators but active elements of the security control logic.

By embedding QoS/QoE evaluation into the adaptive security loop and formalizing their interaction through a unified utility framework, the proposed model provides a mathematically grounded and practically implementable basis for assessing information service quality in distributed networks under adversarial conditions. Its novelty lies not in introducing new isolated metrics, but in recasting security, performance, and experience as inseparable components of a single dynamic system whose behavior can be quantitatively analyzed and optimized in real time.

In order to substantiate the feasibility and internal consistency of the proposed mathematical model, a dedicated software module was developed with the explicit aim of operationalizing the QoS/QoE evaluation process within an adaptive security loop of a distributed network. The implementation was designed not merely as an experimental script, but as a modular analytical framework capable of emulating realistic traffic observation, attack detection, adaptive mitigation, and quality assessment under adversarial conditions.

The program follows a layered architecture in which data acquisition, security analytics, quality evaluation, and decision coordination are logically decoupled yet tightly synchronized, as illustrated in Fig. 1.

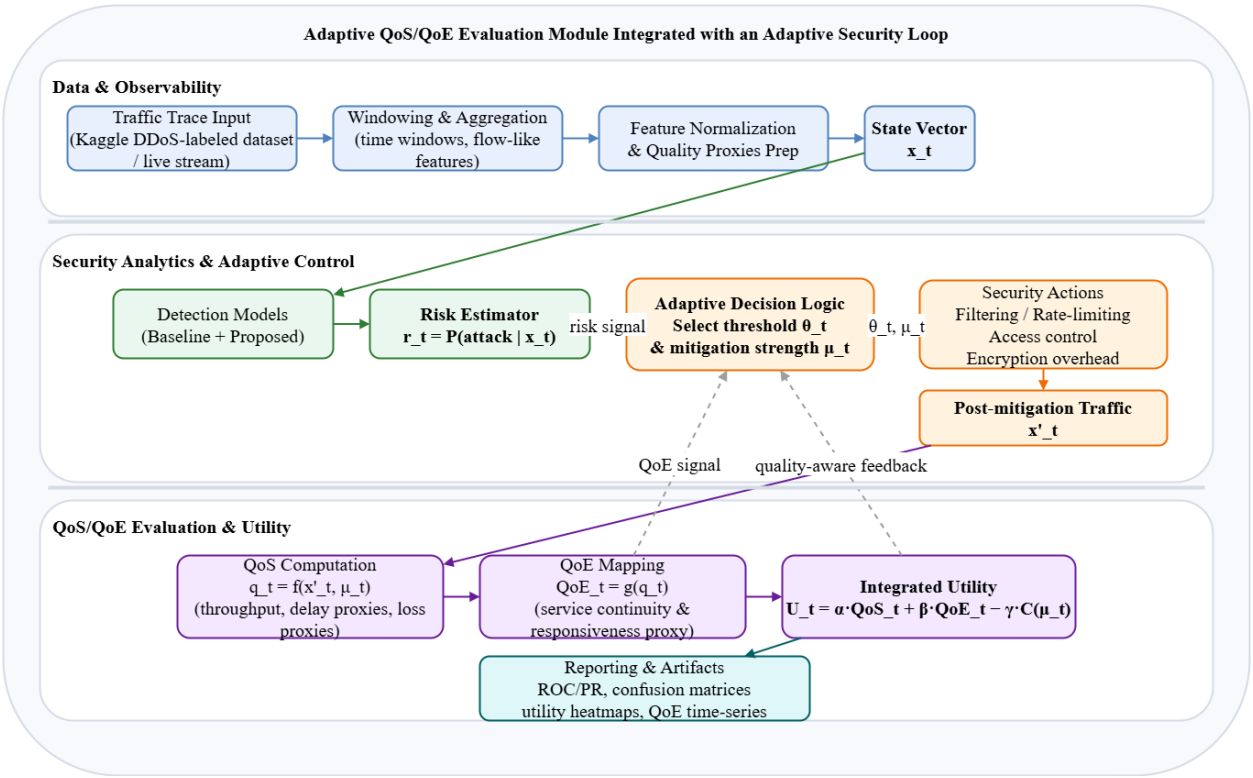

Fig. 1. Architecture of the proposed adaptive QoS/QoE evaluation module

At the lowest layer, the system ingests labeled network traffic traces and aggregates them into fixed-duration temporal windows, thereby transforming raw packet-level information into flow-oriented representations suitable for scalable processing. This aggregation stage mirrors the behavior of distributed monitoring probes, ensuring that subsequent analysis remains computationally tractable even under high traffic volumes.

On top of the data abstraction layer, a detection and risk estimation component is instantiated. This component employs supervised learning models to infer the probability of malicious activity for each observation window, producing a continuous-valued risk signal rather than a binary classification outcome. Such a design choice allows the detection output to be seamlessly integrated into the adaptive security loop, where it serves as a quantitative trigger for subsequent mitigation decisions instead of a rigid alarm. The architecture explicitly supports interchangeable detection backends, enabling the comparison between

conventional baseline classifiers and more expressive ensemble-based models without altering the surrounding evaluation logic.

The core of the implementation is the adaptive control layer, which translates the estimated attack risk into concrete security actions. This layer governs the selection of decision thresholds and mitigation intensity parameters that represent, in an abstracted manner, access control enforcement, traffic filtering, and encryption overhead. These parameters are not applied statically; instead, they are recalculated for each time window, reflecting the evolving network state and perceived threat level. The control logic thus emulates an adaptive security loop in which defensive measures are continuously tuned rather than deployed in a one-size-fits-all fashion.

Parallel to the security control flow, the program incorporates a quality evaluation layer that computes QoS indicators directly from the post-mitigation traffic representation. These indicators are subsequently transformed into a QoE proxy through a nonlinear aggregation function that preserves sensitivity to service degradation while avoiding reliance on application-specific subjective scales. The tight coupling between mitigation parameters and quality assessment ensures that every security decision is immediately reflected in measurable service-level consequences, a property that is central to the proposed evaluation paradigm.

A distinctive feature of the software architecture is the integration of a unified utility computation module, which fuses QoS, QoE, and security overhead into a single evaluative signal. This module enables systematic exploration of the decision space by varying thresholds and mitigation strengths and observing their projected impact on overall system utility. By embedding this computation directly into the execution pipeline, the program facilitates automated sensitivity analysis and supports the identification of operating regimes in which security effectiveness and service quality are jointly optimized.

From an implementation standpoint, the software was developed in Python using a modular design philosophy, with clear separation between data preprocessing, model inference, adaptive control, and visualization components. The program automatically generates diagnostic artifacts, including time-series plots, decision landscapes, and comparative performance diagrams, thereby ensuring that the internal behavior of the adaptive loop remains transparent and reproducible. The overall structure of the system, depicted in Fig. 1, reflects a deliberate effort to align the computational workflow with the conceptual structure of the proposed mathematical model, translating theoretical constructs into executable processes without introducing ad hoc simplifications.

To support the experimental validation of the proposed model, a publicly available labeled network traffic dataset was employed. The study utilized the Network Traffic Dataset for DDoS Detection [13], which contains packet-level records of both benign and malicious network activity. The dataset was collected in a controlled environment using a Kali Linux machine, where normal traffic was generated through typical web browsing behavior, while distributed denial-of-service attacks were synthetically produced using standard traffic generation tools, including ICMP flood, UDP flood, and TCP SYN flood scenarios. Network packets were captured using Wireshark and subsequently converted from PCAP format into a structured CSV representation via Tshark.

The dataset incorporates traffic originating from multiple transport protocols, namely TCP, UDP, and ICMP, and provides a binary label indicating normal operation or attack conditions. Each record includes temporal information, protocol identifiers, packet size attributes, protocol-specific control fields, and source–destination addressing metadata, enabling the extraction of both traffic intensity and structural diversity features. Such characteristics make the dataset particularly suitable for machine learning–based intrusion detection and for analyzing how attack mitigation mechanisms influence network performance indicators.

In the context of this study, the dataset was used not only to train and evaluate attack detection models, but also to emulate realistic traffic dynamics within the adaptive security loop. By aggregating packet-level observations into fixed-duration time windows, the dataset enabled the derivation of QoS-related proxies and the subsequent assessment of their impact on a normalized QoE measure. This approach ensured that the evaluation of service quality was grounded in realistic attack conditions while remaining reproducible and independent of proprietary traffic traces.

In summary, the developed program serves as a concrete instantiation of the proposed QoS/QoE-aware adaptive security framework, providing a technically coherent environment in which the interaction between attack detection, mitigation decisions, and service quality evaluation can be examined under controlled yet realistic conditions.

The experimental evaluation was conducted to assess how the proposed integrated QoS/QoE-aware adaptive security model behaves under realistic attack conditions and how it contrasts with a baseline, security-centric decision strategy. The obtained results consistently demonstrate that embedding quality-awareness into the security control loop leads to more balanced and service-preserving outcomes, even when attack detection performance remains comparable.

The temporal evolution of user-perceived service quality is illustrated in Fig. 2.

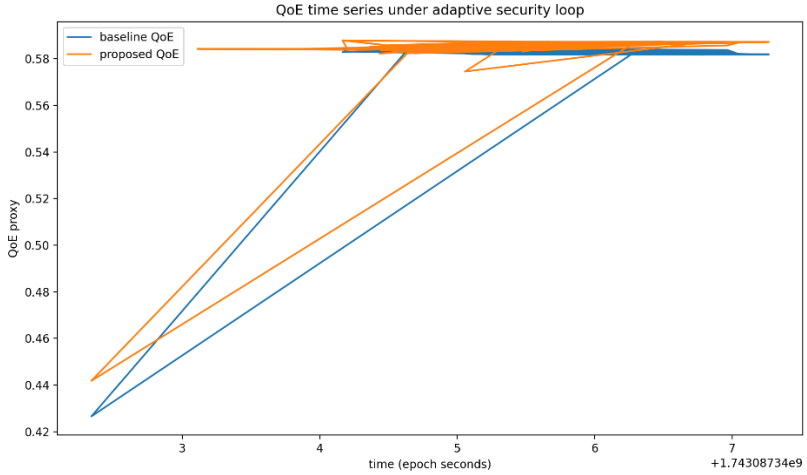

Fig. 2. QoE time series under baseline and proposed adaptive security strategies

The results reveal that while both approaches eventually converge to a similar steady-state QoE level, the proposed model exhibits a noticeably smoother trajectory and a faster stabilization phase. In contrast, the baseline approach shows steeper QoE fluctuations, reflecting abrupt mitigation actions that momentarily degrade service continuity. This behavior indicates that the proposed adaptive loop mitigates attacks in a more graduated manner, avoiding unnecessary overreaction and preserving user experience during transient threat conditions.

The classification capability of the security component is analyzed through receiver operating characteristics shown in Fig. 3.

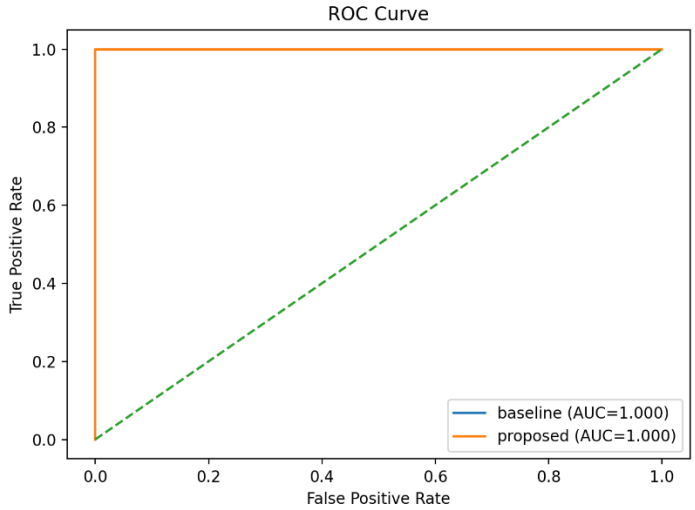

Fig. 3. ROC curves for baseline and proposed detection models

Both approaches achieve near-perfect discrimination between normal and attack traffic, with identical area-under-curve values. This result is essential, as it confirms that the observed differences in service quality are not caused by inferior detection accuracy, but rather by the way detection outputs are operationalized within the adaptive decision process. Hence, the improvement introduced by the proposed model stems from decision coupling rather than raw classification power.

A more nuanced perspective emerges from the analysis of the integrated utility function, visualized in Fig. 4.

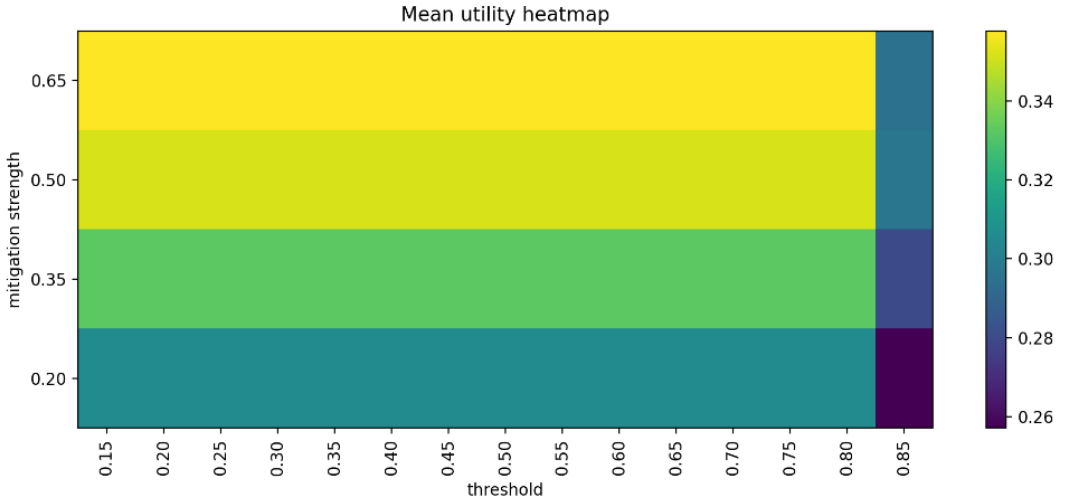

Fig. 4. Mean utility heatmap across decision thresholds and mitigation strengths

The heatmap exposes a broad plateau of high-utility configurations for the proposed model, indicating robustness with respect to parameter tuning. Notably, extreme threshold values or overly aggressive mitigation levels lead to a marked utility decline, which quantitatively confirms the intuitive trade-off between security enforcement and service degradation. The existence of a stable high-utility region demonstrates that the proposed formulation naturally guides the system toward balanced operating regimes instead of brittle, threshold-sensitive configurations.

This observation is further corroborated by Fig. 5, where the utility curve remains nearly flat across a wide threshold interval before dropping sharply at overly conservative settings.

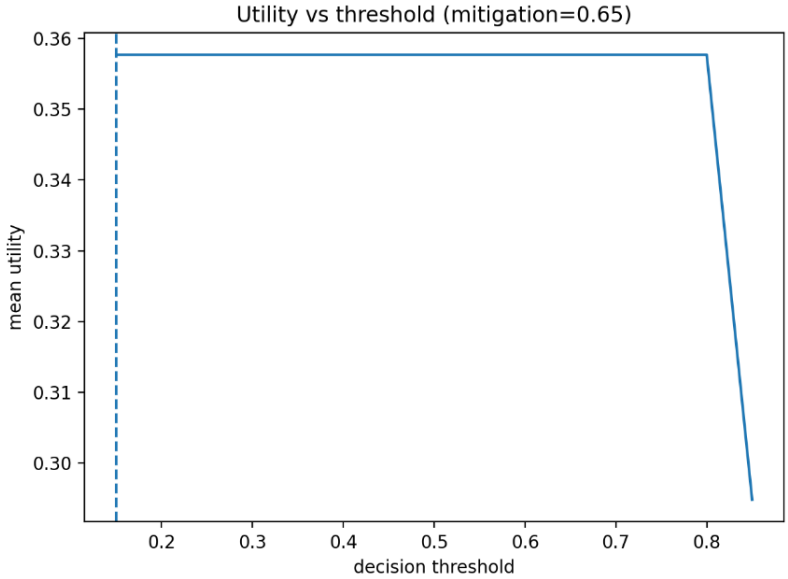

Fig. 5. Utility as a function of decision threshold for fixed mitigation intensity

Such behavior implies that the proposed model tolerates moderate uncertainty in decision calibration without compromising overall system effectiveness, an important property for real-world distributed deployments where precise parameter tuning is rarely feasible.

The confusion matrices presented in Fig. 6 and Fig. 7 highlight subtle yet meaningful differences in classification outcomes.

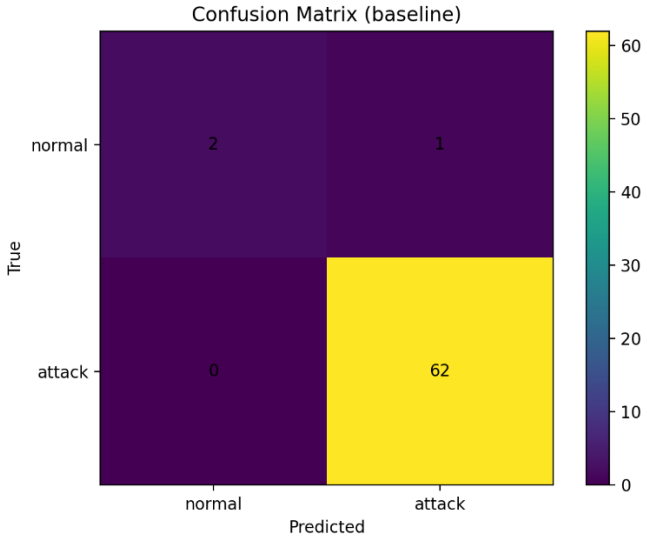

Fig. 6. Confusion matrix for the baseline approach

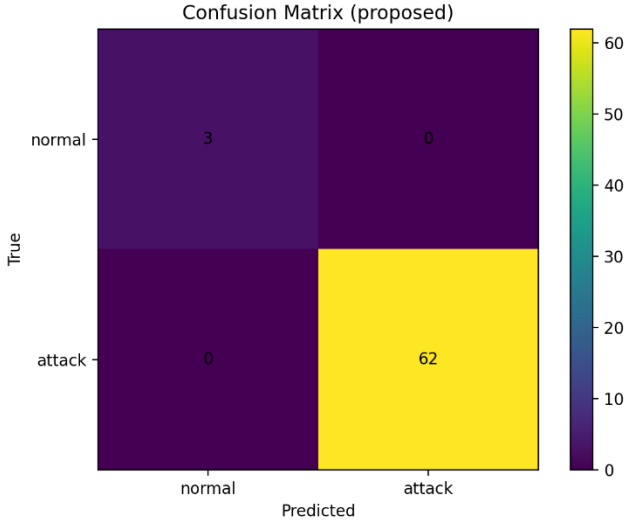

Fig. 7. Confusion matrix for the proposed approach

While both models correctly identify the majority of attack instances, the proposed approach eliminates false alarms on benign traffic entirely. This reduction in false positives is particularly relevant from a QoE perspective, as unnecessary mitigation actions triggered by misclassification directly translate into avoidable service impairment.

To gain insight into the internal decision drivers of the detection component, feature contribution analysis was performed, as shown in Fig. 8.

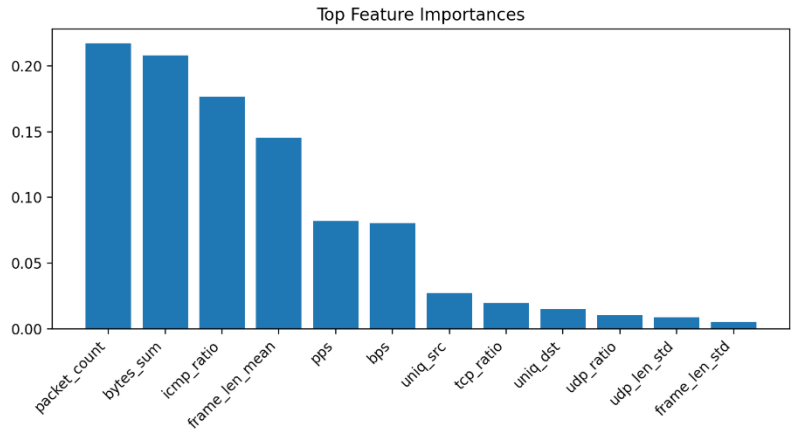

Fig. 8. Top feature importances for attack detection

The dominance of traffic intensity and protocol composition features suggests that the model captures structural characteristics of attack behavior rather than relying on fragile, packet-level artifacts. This property enhances generalization and aligns well with the window-based abstraction adopted in the mathematical formulation.

Finally, the precision-recall characteristics depicted in Fig. 9 confirm that both approaches maintain perfect precision across the full recall range.

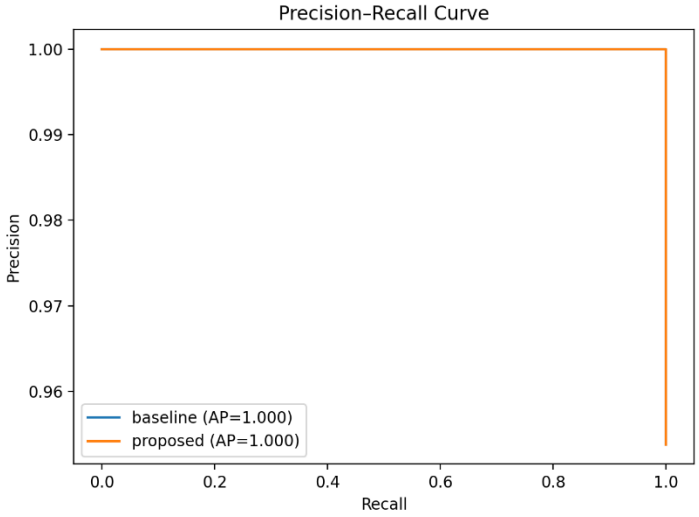

Fig. 9. Precision-Recall curves for baseline and proposed models

From an evaluation standpoint, this result further isolates the contribution of the proposed framework to the adaptive control layer, reinforcing the claim that performance gains are rooted in quality-aware decision orchestration rather than improvements in attack detection alone.

Taken together, the experimental findings directly address the stated objective of the study: to quantitatively assess how security decisions influence service quality and user experience in distributed networks. The results demonstrate that the proposed model fulfills this objective by transforming security enforcement from a purely defensive mechanism into a quality-sensitive control process. By integrating QoS and QoE evaluation into the adaptive security loop, the model achieves a superior balance between protection effectiveness and service preservation, thereby constituting an optimal and practically viable solution for modern distributed information services.

Conclusions and prospects for further research. This study has proposed and validated an integrated QoS/QoE evaluation method that reconceptualizes adaptive security not as an isolated defensive mechanism, but as a quality-sensitive control process embedded within the operational fabric of distributed networks. By formalizing the interaction between traffic dynamics, attack detection, mitigation intensity, and service perception, the developed approach establishes a coherent bridge between measurable network behavior and user-oriented service continuity.

The presented mathematical model introduces a unified utility-based formulation that simultaneously accounts for Quality of Service indicators, Quality of Experience proxies, and security overhead. Unlike conventional multi-metric assessments that remain descriptive or post hoc, the proposed framework enables continuous, real-time evaluation of how security actions reshape service quality. The accompanying software implementation demonstrates that this formulation is not merely conceptual, but can be operationalized using realistic traffic data and machine learning-based detection components. Experimental results confirm that quality-aware adaptation allows the system to preserve user experience more consistently while maintaining equivalent attack detection capability, thereby achieving a more balanced and resilient operating regime.

From a broader perspective, the findings underscore a shift in how security effectiveness should be interpreted in distributed information systems. Rather than maximizing detection accuracy or mitigation aggressiveness in isolation, the results indicate that optimal solutions emerge when security decisions are explicitly constrained and guided by their impact on service utility. This insight is particularly relevant for modern networks characterized by dense edge deployments, multi-domain orchestration, and increasing reliance on automated control loops.

Future research directions naturally extend from the limitations and abstractions of the current study. One promising avenue lies in enriching the QoE modeling layer with service-specific perception functions derived from application telemetry or user feedback, enabling finer-grained differentiation between heterogeneous information services. Another direction involves integrating predictive elements into the adaptive loop, allowing the system to anticipate quality degradation under evolving attack patterns rather than reacting solely to instantaneous observations. Additionally, extending the framework to multi-tenant and multi-operator environments would allow investigation of accountability, fairness, and cross-domain utility optimization under shared infrastructure constraints.

In summary, the proposed integrated QoS/QoE evaluation method provides a principled and extensible foundation for quality-aware security management in distributed networks. By aligning protection mechanisms with service-level outcomes and user experience considerations, it opens a pathway toward more intelligent, transparent, and sustainable operation of future information services.

References

1. QoE-aware edge server placement in mobile edge computing using an enhanced genetic algorithm / J. Sha et al. *International Journal of Intelligent Networks*. 2025. Vol. 6. P. 65–78. URL: https://doi.org/10.1016/j.ijin.2025.07.003.
2. Security, QoS and energy aware optimization of cloud-edge data centers using game theory and homomorphic encryption: Modeling and formal verification / M. Marwan et al. *Results in Engineering*. 2024. P. 102902. URL: https://doi.org/10.1016/j.rineng.2024.102902.
3. Dhandapani M., Vetriselvi V., Aishwarya R. CoopAI-Route: DRL Empowered Multi-Agent Cooperative System for Efficient QoS-Aware Routing for Network Slicing in Multi-Domain SDN. *Computer Modeling in Engineering & Sciences*. 2024. P. 1–10. URL: https://doi.org/10.32604/cmes.2024.050986.
4. Barakabitze A. A., Walshe R. SDN and NFV for QoE-driven multimedia services delivery: The road towards 6G and beyond networks. *Computer Networks*. 2022. P. 109133. URL: https://doi.org/10.1016/j.comnet.2022.109133.
5. Shaji N. S., Muthalagu R. Survey on security aspects of distributed software-defined networking controllers in an enterprise SD-WLAN. *Digital Communications and Networks*. 2023. URL: https://doi.org/10.1016/j.dcan.2023.09.004.
6. Service Level Agreement in cloud computing: Taxonomy, prospects, and challenges / F. Qazi et al. *Internet of Things*. 2024. P. 101126. URL: https://doi.org/10.1016/j.iot.2024.101126.
7. Edge computing in future wireless networks: A comprehensive evaluation and vision for 6G and beyond / M. Ergen et al. *ICT Express*. 2024. URL: https://doi.org/10.1016/j.icte.2024.08.007.
8. Ibrahim AlShathri S., S. M. Hassan D., Allaoua Chelloug S. Latency-Aware Dynamic Second Offloading Service in SDN-Based Fog Architecture. *Computers, Materials & Continua*. 2023. Vol. 75, no. 1. P. 1501–1526. URL: https://doi.org/10.32604/cmc.2023.035602.
9. Optimal Deploying IoT Services on the Fog Computing: A Metaheuristic-Based Multi-Objective Approach / B. Wu et al. *Journal of King Saud University - Computer and Information Sciences*. 2022. URL: https://doi.org/10.1016/j.jksuci.2022.10.002.
10. Mobility-aware fog computing in dynamic networks with mobile nodes: A survey / K. Ostrowski et al. *Journal of Network and Computer Applications*. 2023. P. 103724. URL: https://doi.org/10.1016/j.jnca.2023.103724.
11. VWA-6G AI assisted continuous security monitoring over open RAN service management orchestration / Y.-C. Tung та ін. *Computers & Security*. 2025. С. 104566. URL: https://doi.org/10.1016/j.cose.2025.104566.
12. On resource consumption of machine learning in communications network security / M. M. Hoque et al. *Computer Networks*. 2025. No. 271. 111600. URL: https://doi.org/10.1016/j.comnet.2025.111600.
13. Network Traffic Dataset for DDoS Detection. *Kaggle*. URL: https://www.kaggle.com/datasets/shaikmubeen/network-traffic-dataset-for-ddos-detection.

Історія статті:
Отримано: 12.02.2026 Доопрацьовано: 03.03.2026 Прийнято до друку: 23.03.2026 Опубліковано: 29.03.2026