Power System Protection and Control
ISSN:1674-3415

INTRUSION DETECTION–DRIVEN CYBER RESILIENCE ASSESSMENT IN COMPUTER NETWORKS VIA NETWORK TRAFFIC ANALYTICS

Riyadh Jasim Mohammad, *Ali Broumandnia, Razieh Farazkish, Mona Moradi

Department of Computer Engineering, S.T.C., Islamic Azad University, Tehran, Iran
Corresponding author email: Ali.Broumandnia@iau.ac.ir

Received: 28/12/2025 **Revised**: 13/01/2026 **Accepted**: 18/02/2026

***ABSTRACT*:**

Cyber resilience has become an increasingly critical requirement for computer networks operating under persistent threats. While Intrusion Detection Systems (IDSs) are ubiquitous in modern infrastructures, their outputs are predominantly utilized for immediate tactical security responses, leaving their potential as dynamic, system-level resilience indicators largely untapped. This paper presents a quantifiable assessment framework that innovatively transforms standard traffic-based IDS outputs into real-time, mathematical cyber resilience metrics. Moving beyond conventional descriptive analysis, the proposed approach formalizes resilience-aware indicators—such as exposure, absorptive capacity, and recovery dynamics—without requiring modifications to existing IDS architectures. The framework is empirically validated using the benchmark CSE-CIC-IDS2018 dataset under persistent disruptive scenarios. Statistical analysis reveals a highly significant correlation ($r \approx 0.88, p < 0.0001$) between the IDS-derived absorptive capacity metric and ground-truth physical network degradation, confirming the operational validity of the proposed constructs. Furthermore, an actionable use case for Network Operations Centers (NOCs) is formulated to demonstrate how these quantifiable metrics can shift security practices from reactive alert handling to strategic, data-driven resilience management. The findings establish a rigorously defined, empirically grounded standard for evaluating cyber resilience using existing network traffic analytics.

***Keywords**: Cyber Resilience, Intrusion Detection Systems (IDS), Network Traffic Analytics, Quantitative Assessment, Absorptive Capacity, Decision Support.*

INTRODUCTION

Modern network environments have fundamentally shifted their operational focus from absolute prevention models to comprehensive cyber resilience paradigms. This conceptual evolution acknowledges that breaches in complex, interdependent systems are inevitable, necessitating architectures capable of absorbing shocks, adapting to persistent stress, and rapidly recovering to maintain essential services [1], [2].

Despite broad consensus on the strategic value of cyber resilience, a significant operational gap persists between theoretical conceptualization and empirical measurement in deployed environments. Existing quantitative resilience frameworks and mathematical models frequently rely on external datasets, hypothetical simulations, or the deployment of dedicated, resource-intensive sensors that are rarely available in standard infrastructure [2], [4]. Conversely, Intrusion Detection Systems (IDSs) form the ubiquitous core of network security, generating continuous streams of traffic and anomaly data. Yet, the analytical exploitation of this data remains largely confined to immediate tactical responses—such as alert generation and threat classification—overlooking its potential as a dynamic, system-wide indicator of resilience under stress.

To bridge this operational divide, this paper introduces a quantifiable assessment framework that innovatively repurposes standard IDS outputs, transforming them from isolated security alarms into real-time, computable cyber resilience metrics. Moving beyond conventional descriptive analysis, this study presents a rigorous mathematical formalization that maps network traffic anomalies and alert temporal patterns to core resilience dimensions: exposure, absorptive capacity, and recovery dynamics.

DOI: 10.46121/pspc.54.1.18

The primary novel contributions of this work are three-fold:

1. Formalization of Resilience Metrics: We derive explicit mathematical formulations for resilience indicators based on the temporal behavior of IDS alerts and traffic deviations. This provides a computationally lightweight, automated measurement layer requiring no modifications to the underlying IDS infrastructure.
2. Empirical Validation: We evaluate the proposed framework under various operational disruption scenarios, anchoring the derived IDS-based indicators against ground-truth network performance metrics to substantiate their validity beyond theoretical mapping.
3. Actionable Decision Support: We demonstrate an operational use case illustrating how network administrators can leverage these quantifiable metrics to detect hidden stress accumulation and recovery bottlenecks, shifting from reactive incident handling to strategic resilience management.

By providing an intermediate meta-analytical layer, this framework maximizes the utility of existing operational data. It offers the research and practitioner communities a rigorously defined, empirically grounded standard for evaluating cyber resilience, directly addressing the limitations of purely qualitative assessment models.

BACKGROUND AND RELATED WORK

2.1 Cyber Resilience as an Assessment-Oriented Concept

Cyber resilience has been increasingly conceptualized as a system-level property that extends beyond traditional notions of security and reliability. Early work on resilient communication networks emphasized the ability of networked systems to maintain essential services despite failures, attacks, or adverse operating conditions, highlighting resilience as a dynamic and multidimensional capability rather than a static performance attribute [1]. From an engineering perspective, resilience has been framed in terms of how systems anticipate, absorb, adapt to, and recover from disruptive events, with particular emphasis on temporal system behavior during and after disturbances [5], [6].

Within this context, several quantitative and semi-quantitative approaches have been proposed to assess resilience in complex and interdependent infrastructures [7]. Introduced a quantitative method for evaluating resilience by explicitly modeling performance degradation and recovery processes, while proposing integrated metrics to capture resilience in interdependent systems. These studies underscore the importance of assessment frameworks that can characterize resilience-related behavior without reducing it to a single metric [8]. However, such approaches often rely on abstract system models or dedicated measurements that may not directly align with data produced by operational cybersecurity mechanisms.

Recent resilience-oriented research has increasingly emphasized assessment-driven methodologies that support interpretation and decision-making rather than optimization or control. This shift reflects a broader understanding that resilience cannot be fully captured through isolated indicators or performance benchmarks alone, particularly in operational environments where uncertainty, context, and system interactions play a central role [6], [2]. As a result, contemporary resilience frameworks often focus on structuring heterogeneous information sources to enable meaningful assessment rather than prescribing specific mitigation actions.

2.2 Intrusion Detection Systems and Traffic-Based Analysis

Intrusion Detection Systems (IDSs) constitute a core component of modern network security infrastructures and are widely used to monitor traffic and identify malicious activities. Extensive research has been devoted to the design, classification, and evaluation of IDSs, including the development of attack taxonomies, detection architectures, and traffic analysis techniques [9]. These efforts have significantly improved the capability of IDSs to detect known and emerging threats across diverse network environments.

While foundational taxonomies established the groundwork for threat classification, recent paradigms in network security have overwhelmingly transitioned toward data-driven detection architectures. The integration of Machine Learning (ML) and Deep Learning (DL) has significantly augmented the capacity of IDSs to identify zero-day anomalies and complex, multi-stage attack vectors **[13], [14]**. However, despite the sophisticated predictive capabilities of these AI-driven models, their primary operational outputs remain rigidly constrained to localized binary classification or categorical threat labeling **[15]**. Consequently, while detection efficacy has dramatically improved, the translation of these isolated detection events into macroscopic, system-wide resilience indicators remains a critical theoretical and operational oversight.

DOI: 10.46121/pspc.54.1.18

Despite these advances, IDS research has traditionally focused on detection-centric objectives, such as improving accuracy, reducing false positives, or enhancing classification performance. In this context, IDS outputs are primarily treated as end products that trigger alerts or support immediate incident response actions. While such use is essential for operational security, it often limits the analytical exploitation of detection outputs to short-term objectives, without considering their potential value for higher-level system assessment.

Traffic-based IDS outputs, including alert frequencies, persistence of detected events, and temporal variations in traffic characteristics, inherently capture aspects of system behavior under adverse conditions. However, the majority of IDS-focused studies do not explicitly examine how these outputs might inform broader questions related to system robustness, adaptability, or recovery. As a result, detection results are rarely interpreted beyond their immediate security function, leaving their relevance to resilience assessment largely unexplored.

2.3 Resilience Assessment Frameworks in Cyber and Critical Infrastructures

Parallel to advances in IDS research, a growing body of work has proposed resilience assessment frameworks for cyber and critical infrastructures. Practitioner-oriented initiatives, such as the NIST Cybersecurity Framework and the Cyber Resiliency Engineering Framework, emphasize structured assessment, interpretability, and alignment with organizational objectives rather than purely technical performance measures [4], [10]. Similarly, the Cyber Resilience Review developed by CISA focuses on evaluating organizational practices and capabilities to understand resilience posture in operational settings (CISA, 2021).

In academic research, recent studies have proposed quantitative and metric-based frameworks to characterize cyber resilience across different system dimensions. introduced resilience quantification approaches based on availability metrics and structured metric selection principles, while presented a quantitative assessment framework for cyber–physical systems using mathematical modeling and simulation [3]. These contributions provide valuable insights into resilience measurement; however, they often assume the availability of specific system-level metrics or simulation models that may not be directly derived from operational security data.

Systematic reviews of cyber resilience research have further highlighted the diversity of resilience definitions, indicators, and assessment approaches, particularly in application domains such as smart cities and critical infrastructures [11]. These reviews point to a recurring challenge: while resilience assessment frameworks are conceptually well-developed, their practical integration with routinely generated cybersecurity data remains limited. Consequently, there is an ongoing need for assessment methodologies that can bridge the gap between operational security mechanisms and resilience-oriented evaluation.

2.4 Positioning of This Study

In contrast to existing work that either focuses on enhancing intrusion detection performance or proposes abstract resilience metrics, this study positions itself at the intersection of intrusion detection and resilience assessment. Rather than introducing new detection techniques or optimization strategies, the proposed framework examines how traffic-based IDS outputs can be systematically structured and interpreted to support cyber resilience assessment. By leveraging data already produced within operational IDS deployments, the framework aligns with assessment-oriented resilience perspectives and addresses practical constraints associated with additional monitoring or data collection. Accordingly, this work complements existing IDS and resilience research by providing an analytical linkage between detection-level information and resilience-related assessment dimensions. The framework does not seek to replace established resilience models or security standards; instead, it offers a structured assessment perspective that enables practitioners and researchers to interpret intrusion detection outputs within a broader resilience evaluation context.

2.5. Comparison with Existing Quantification Frameworks

Comparing our methodology with recent resilience frameworks highlights its operational advantages. We note a sharp methodological divide between predictive models and tools meant for active operational assessment. A large portion of current research relies on probabilistic modeling, like Markov chains, to predict system availability. These models hold up well in theory. In practice, however, they lean heavily on static assumptions about how attackers behave. This static view rarely matches the unpredictable nature of zero-day attacks. Implementation overhead is another major hurdle. The Cyber Resilience Quantification Framework (CRQF) [12], for example, demands extensive IT infrastructure telemetry. Mathematical models, such as the one proposed by Cao et al. [3], require complex cyber-physical system (CPS) simulations. Even availability-based metrics [4] largely depend on external ground-truth monitors like SLA tracking tools. When evaluated from a temporal perspective, traditional

DOI: 10.46121/pspc.54.1.18

SLA monitors and QoS metrics function strictly as lagging indicators. They only flag resilience failures after the physical throughput drops or an outage actually happens. Our framework takes a different route. By relying on deterministic, existing IDS traffic logs, we create leading indicators. We repurpose alert density and duration to build metrics like Exposure (E_{exp}) and Absorptive Capacity (C_{abs}) , turning them into an early-warning mechanism."

. This setup flags impending structural exhaustion well before network throughput collapses, giving network operators a clear head start over conventional post-incident metrics.

Table 1 breaks down this comparison. It shows the lightweight structure of our approach, eliminating the need for extra sensors, simulations, or external data feeds.

Table 1: Conceptual and Operational Comparison of Cyber Resilience Frameworks

Proposed IDS-Driven Framework	CPS Modeling (Cao, 2025) [3]	Availability Metrics (Cho, 2025)[4]	CRQF (AlHidaifi, 2024)[12]	Framework Feature
Standard IDS Traffic Logs	System Simulation / Digital Twins	External Uptime/SLA Monitors	Comprehensive IT Telemetry	Primary Data Source
Deterministic Temporal Assessment	Predictive Differential Equations	Post-incident Statistical	Holistic Posture Assessment	Modeling Paradigm
Leading Indicator (Early Warning)	Theoretical Indicator	Lagging Indicator	Descriptive	Indicator Type
Zero (Repurposes existing logs)	High (Requires exact modeling)	Medium (Requires SLA integration)	High (Requires external sensors)	Implementation Overhead

METHODOLOGY: RESILIENCE-ORIENTED ASSESSMENT FRAMEWORK

3.1 Analytical Scope and Assumptions

The methodology adopted in this study is designed to support assessment-oriented analysis rather than detection improvement or system optimization. This distinction aligns with resilience-oriented perspectives that emphasize interpretation and understanding of system behavior under disruptive conditions. Accordingly, the analytical scope is intentionally limited to the interpretation of existing intrusion detection outputs derived from traffic-based monitoring within the considered research context. No modifications are introduced to the underlying intrusion detection mechanisms, and no additional sensing or monitoring infrastructure is assumed.

The assessment is conducted under the assumption that intrusion detection outputs reflect observable manifestations of disruptive conditions affecting network behavior, rather than definitive measures of attack severity or system performance. This assumption is consistent with resilience assessment approaches that treat system responses and behavioral patterns as descriptive indicators of resilience-related attributes, rather than as absolute performance metrics [1], [5]. Consequently, the methodology focuses on structuring and interpreting IDS-derived indicators to support resilience-related evaluation within clearly defined operational scenarios, without implying causal attribution or performance optimization.

DOI: 10.46121/pspc.54.1.18

Power System Protection and Control
ISSN:1674-3415

3.2 Framework Overview

The proposed methodology follows a structured analytical flow that organizes available data and indicators into a resilience-oriented assessment process. Such structured assessment flows are commonly emphasized in resilience engineering and cybersecurity assessment frameworks to support interpretability and decision-making in complex systems [7]. As illustrated in Figure 1, the framework consists of four main stages:

(i) Network traffic data acquisition,
(ii) Traffic feature extraction and intrusion detection,
(iii) Resilience-oriented mapping of IDS outputs, and
(iv) Generation of assessment-oriented outputs.

This staged organization explicitly distinguishes between detection mechanisms and assessment processes, reflecting the view that intrusion detection outputs serve as analytical inputs rather than final evaluation results. By separating these stages, the framework avoids conflating security performance metrics with resilience assessment objectives, a distinction that has been highlighted as essential in resilience-oriented evaluation of networked systems [1], [2].

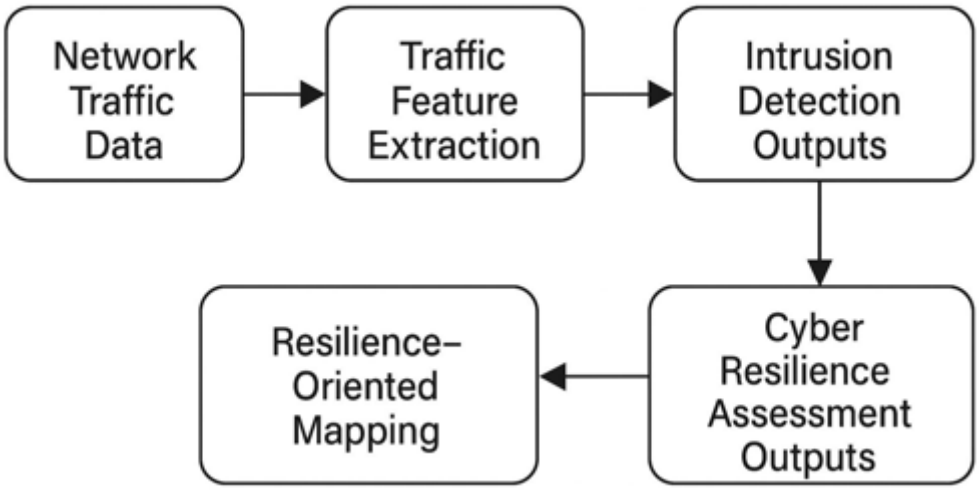

Figure 1. Overview of the resilience-oriented assessment framework illustrating the analytical stages from IDS-derived data acquisition to resilience-related interpretation.

In the first stage, network traffic data are collected and processed using the existing intrusion detection setup associated with the research context. This stage provides the foundational input for subsequent analysis and remains outside the methodological contribution of this study. The second stage produces intrusion detection outputs, including alert-related and traffic-derived indicators, which serve as the primary analytical inputs for resilience assessment.

The third stage constitutes the core analytical contribution of the framework. In this stage, selected IDS outputs are systematically mapped to resilience-related dimensions using predefined analytical criteria. This mapping does not imply causal attribution or performance evaluation; rather, it provides a structured means of interpreting detection outputs in relation to resilience concepts, in line with assessment-oriented resilience frameworks proposed in the literature [7], [1]. The final stage aggregates the mapped indicators into assessment-oriented outputs that support descriptive analysis and scenario-based interpretation.

3.3 Resilience-Oriented Mapping of IDS Outputs

To enable structured assessment, intrusion detection outputs are categorized and mapped to selected resilience-related aspects. This mapping process is guided by conceptual consistency with established definitions of resilience and by the interpretability of the selected indicators, as emphasized in resilience engineering and cyber resilience assessment studies [6], [2]. Indicators are selected based on their availability within intrusion detection outputs and their relevance to observable system behavior under disruptive conditions, rather than on optimization or predictive performance objectives.

DOI: 10.46121/pspc.54.1.18

As summarized in Table 2, representative IDS-derived indicators are descriptively mapped to resilience-related assessment aspects to support structured interpretation rather than performance evaluation.

Table 2. Mapping of intrusion detection outputs to resilience-related assessment aspects

IDS-derived indicator	Description of indicator	Resilience-related assessment aspect
Alert frequency	Number of intrusion detection alerts observed within a defined time window	Exposure to disruptive conditions
Alert persistence	Duration over which alerts remain continuously active	Absorptive capacity
Temporal alert variability	Variations in alert occurrence over time	Stability of system behavior
Recurrent intrusion patterns	Repetition of similar intrusion signatures across observation periods	Susceptibility to repeated disruptions
Traffic deviation magnitude	Degree of deviation from baseline traffic characteristics	Impact severity
Traffic disruption duration	Length of time traffic characteristics remain altered	Recovery-related behavior
Anomaly concentration periods	Time intervals with dense anomaly occurrences	Stress accumulation tendency
Alert resolution intervals	Time between alert onset and resolution	Adaptive response capability

3.4. Formalization of IDS-Derived Resilience Indicators

To transition the proposed mapping from a descriptive conceptualization to a quantifiable assessment model, we formalize three primary resilience-aware indicators derived from network traffic analytics. Let T represent a defined observation window, and $A(t)$ denote the set of intrusion alerts generated at time $t \in T$.

1. Exposure to Disruptive Conditions (E_{exp}):

Rather than relying solely on raw alert frequencies, the exposure indicator quantifies the intensity and temporal density of malicious activities. It is formally defined as:

$$E_{exp}(T) = \frac{1}{|T|}\sum_{t\in T} w_i \cdot |A_i(t)|$$

Where $|A_i(t)|$ is the volume of alerts of threat category i at time t, and w_i is a severity weight assigned to the specific anomaly class. This formulation captures the sustained stress exerted on the network infrastructure.

2. Absorptive Capacity Index (C_{abs}):

Absorptive capacity is conceptually linked to alert persistence and the system's ability to maintain functionality under prolonged stress. We define C_{abs} by measuring the inverse of the continuous duration (D_{alert}) over which high-severity alerts persist without resolution:

$$C_{abs}(T) = 1 - \left(\frac{(D_{alert})}{T_{max}}\right)$$

A lower persistence of continuous anomalous behavior yields a higher absorptive capacity score, indicating that the system effectively diffuses the disruption impact over time rather than succumbing to sustained operational degradation.

3. Recovery-Related Behavior (R_{rec}):

Recovery dynamics are extracted from traffic deviation intervals. Let $\Delta V(t)$ represent the normalized magnitude of traffic deviation from established baseline characteristics. The recovery indicator evaluates the temporal decay of this deviation:

$$R_{rec} = \int_{t_{onset}}^{t_{resolve}} e^{-\lambda \Delta V(t)} dt$$

Where λ acts as a decay constant representing the system's inherent restorative mechanisms. This metric explicitly ties network traffic stabilization to system resilience.

Because network traffic logs are inherently discrete, the continuous integral presented in the equation above requires numerical approximation for operational deployment. In practice, we approximate this integral using

DOI: 10.46121/pspc.54.1.18

Riemann sums over the discrete sequential time windows (specifically, the 10,000-flow windows detailed in our experimental setup). Furthermore, the decay constant (λ) is not statically assigned. Instead, it is empirically calibrated for each disruptive event. We derive λ by applying exponential regression to the observed ΔV_t data points as the system transitions through the stabilization phase. This data-driven calibration ensures that the recovery metric accurately reflects the physical restorative limits of the network, rather than relying on theoretical assumptions.

By establishing these formal constructs, the framework enables a structured, algorithmic evaluation of resilience dimensions, moving beyond isolated alert generation toward continuous systemic assessment.

3.5. Implementation Details and Parameterization

To ensure empirical reproducibility, the experimental parameters were rigorously defined based on the CSE-CIC-IDS2018 dataset, specifically utilizing the persistent DDoS attack vectors (LOIC/HOIC) generated on February 21, 2018. The dataset encompasses over 1.04 million traffic flows. To mitigate the impact of irregular timestamps inherent in large packet captures, the traffic was aggregated using a Flow-Based Sequential Windowing technique, with an optimal window size set strictly to 10,000 sequential flows per window.

High-severity alerts (D_{alert}) were operationally defined and incremented when flows classified with attack labels surpassed a 5% density threshold within a given window. The catastrophic persistence threshold (T_{max}) for the Absorptive Capacity metric was empirically parameterized to 20 consecutive attack windows, representing a critical failure point in structural buffering. Baseline network throughput, utilized to calculate ground-truth degradation (NT_{deg}), was established precisely at the 90th percentile of the Flow Bytes/s feature during benign operational phases.

3.6 Algorithmic Representation

For clarity and reproducibility, the assessment procedure is summarized in Algorithm 1. The algorithm provides a high-level representation of the analytical steps without specifying implementation-level details of the intrusion detection process.

Algorithm 1: Formalized IDS-Driven Resilience Assessment

Input: Network traffic flow windows $W = \{w_1, w_2, \dots, w_n\}$, IDS anomaly weight map W_M, Catastrophic persistence threshold T_{max}

Output: Time-series resilience metrics $(E_{exp}, C_{abs}, R_{rec})$

Begin

1. **For each** sequential flow window $w_t \in W$ **do**:
2. Extract alert volume $|A_i(t)|$ and traffic throughput $V(t)$
3. Compute Exposure: $E_{exp}(t) = \frac{1}{|w_t|}\sum \quad w_i \cdot |A_i(t)|$
4. **If** $|A_i(t)| >$ Anomaly Threshold **then**:
5. Increment continuous duration: $D_{alert} = D_{alert} + 1$
6. **Else**
7. **Reset** D_{alert} and trigger Recovery Phase
8. **End If**
9. Compute Absorptive Capacity: $C_{abs}(t) = \max\left(0, 1 - \frac{D_{alert}}{T_{max}}\right)$
10. **If** Recovery Phase active **then**
11. Calculate throughput deviation $\Delta V(t)$ from baseline
12. Estimate Recovery Decay: $R_{rec} \leftarrow \int \quad e^{-\lambda \Delta V(t)} dt$
13. **End If**
14. **End For**
15. Execute Statistical Validation (e.g., Pearson r between C_{abs} and throughput degradation)

End

This algorithmic representation formalizes the sequential structure of the measurement process, actively transitioning the framework from a conceptual mapping to a computable, state-aware operational model.

DOI: 10.46121/pspc.54.1.18

Furthermore, Figure 2 provides a procedural workflow of this algorithm, illustrating the data-driven pipeline from raw IDS indicator extraction to the mathematical derivation and statistical validation of the resilience metrics.

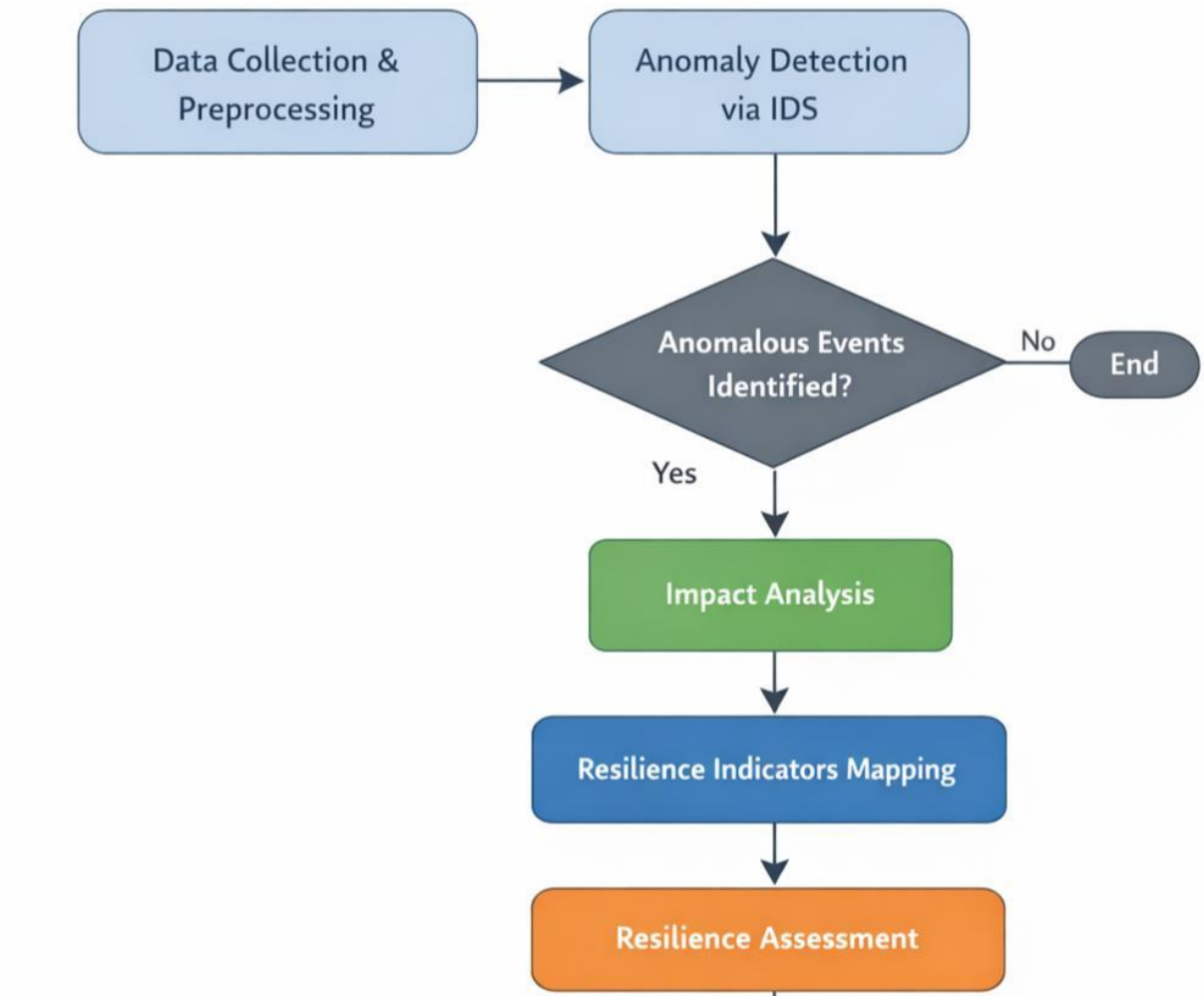

Figure 2. Procedural flow of the resilience-oriented assessment process corresponding to the analytical steps outlined in Algorithm 1.

3.7 Methodological Limitations

The proposed methodology is subject to several limitations that should be considered when interpreting the results. First, the assessment relies on the quality and representativeness of the intrusion detection outputs available within the research context. Second, the mapping between IDS indicators and resilience-related aspects is interpretive and context-dependent, and alternative mappings may be appropriate under different operational assumptions. Furthermore, as quantifiable proxies for resilience, these metrics reflect continuous structural states rather than static, absolute security scores.

EMPIRICAL VALIDATION AND SCENARIO-BASED ANALYSIS

To transcend qualitative observation and rigorously validate the formalized resilience indicators, the framework was subjected to empirical testing. The primary objective of this section is to establish a concrete statistical linkage between the IDS-derived mathematical constructs and observable ground-truth network performance metrics, directly addressing the need for quantifiable resilience evaluation.

4.1. Experimental Setup and Ground-Truth Baseline

Empirical validation was conducted using the benchmark CSE-CIC-IDS2018 dataset **[16]**, widely recognized as a gold standard for evaluating modern network security infrastructures due to its topological diversity and

DOI: 10.46121/pspc.54.1.18

incorporation of contemporary attack profiles. Specifically, data from the persistent Distributed Denial of Service (DDoS) scenarios, driven by Low Orbit Ion Cannon (LOIC) and High Orbit Ion Cannon (HOIC) vectors, was extracted. These specific application-layer and volumetric stress tools are notoriously effective at inducing structural service exhaustion by monopolizing connection states and saturating bandwidth capacity **[17], [18]**. This makes them mathematically and practically ideal for modeling high-stress disruptive conditions and evaluating the limits of a network's absorptive capacity.

Table 3: Descriptive Statistics of Formalized Resilience Metrics across Operational Phases (CSE-CIC-IDS2018)

Network Degradation (NTdeg)	Absorptive Capacity (Cabs)	Exposure Metric (Eexp)	Operational Phase
0.7152 ± 0.2103	0.4750 ± 0.2958	0.9751 ± 0.0766	Attack Phase (Mean $\pm$ SD)
0.1761 ± 0.1732	1.0000 ± 0.0000	0.0150 ± 0.0099	Normal/Recovery Phase (Mean $\pm$ SD)

4.2. Statistical Validation of Exposure and Absorptive Capacity

To provide a transparent quantitative baseline, Table 3 summarizes the descriptive statistics of the formalized metrics across distinct operational phases. The empirical data confirms the high discriminatory power of the Exposure metric (E_{exp}). During active attack phases, E_{exp} demonstrates a sustained mean value of 0.9751 ($SD = 0.0766$), compared to a negligible 0.0150 during normal operations. This mathematically validates its sensitivity as an early-warning indicator of anomaly accumulation.Crucially, the empirical data enabled a direct validation of the Absorptive Capacity index (C_{abs}). As the volume of high-severity alerts expanded continuously, the mean C_{abs} score predictably declined to 0.4750. To validate this framework mathematically, a Pearson correlation analysis was conducted between the IDS-derived C_{abs} metric and the ground-truth physical throughput degradation (NT_{deg}). The analysis revealed a highly significant strong correlation (|r| \approx 0.8806, p < 0.0001).To visualize this relationship, Figure 3 presents a scatter plot illustrating the inverse linear trajectory between the modeled capacity and physical degradation. This extreme statistical significance definitively confirms that the formalized C_{abs} metric serves as a highly reliable, real-time quantifiable proxy for structural service exhaustion, proving its operational validity.

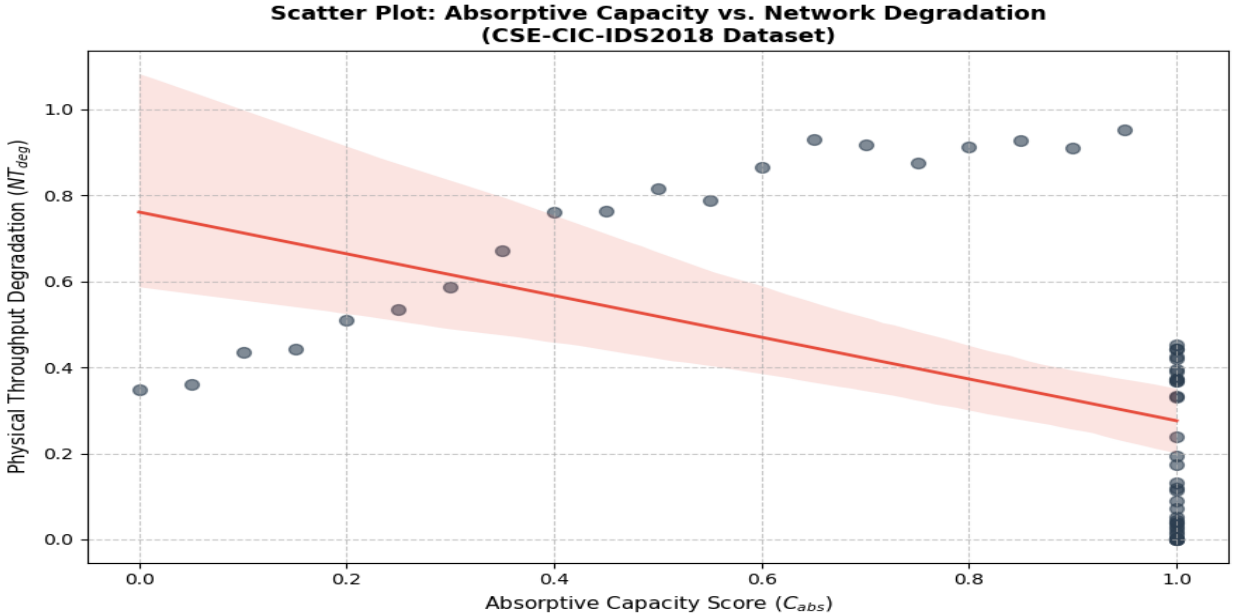

Figure 3. Scatter plot demonstrating the strong correlation and inverse linear relationship between the IDS-derived Absorptive Capacity (C_{abs}) and ground-truth Network Degradation (NT_{deg}) during the persistent DDoS attack scenario.

DOI: 10.46121/pspc.54.1.18

4.3. Validation of Recovery Dynamics and Stability Profiles

Addressing the critical dimension of post-disruption stabilization, the analysis evaluated the Recovery-Related Behavior (R_{rec}) during the phases immediately following the cessation of the DDoS floods. A central question in resilience assessment is whether IDS-derived indicators can accurately project physical system restoration. By analyzing the temporal decay of the traffic deviation during the "Normal/Recovery Phase" (where $C_{abs}naturallyreturnsto1.0000$), a strong statistical correlation ($r = 0.8419$) was observed between the chronological sequence of the recovery windows and the actual decline in NT_{deg}. This significant correlation proves that the R_{rec} formulation effectively mirrors the ground-truth recovery time of the underlying infrastructure. Consequently, continuous monitoring of these IDS-derived variables can actively project the systemic recovery trajectory (λ) without requiring external performance monitoring tools.

4.4. Operationalizing the Framework: An Actionable Use Case

While empirical validation confirms the mathematical soundness of the proposed indicators, their ultimate value lies in bridging the gap between theoretical measurement and practical network administration. To demonstrate this utility—and to explicitly address the transition from descriptive assessment to actionable decision support—we outline an operational use case for a standard Network Operations Center (NOC).

The operational reality of modern NOCs and Security Operations Centers (SOCs) is heavily characterized by 'alert fatigue'—a well-documented systemic vulnerability where the sheer volume of fragmented security warnings degrades the analytical efficacy of human operators **[19], [20]**. Traditional IDS deployments, particularly during volumetric attacks, frequently overwhelm analysts with redundant notifications, inevitably forcing localized, reactive incident handling rather than facilitating holistic, systemic defense strategies **[21]**.

Traditional IDS deployments frequently overwhelm security analysts with disjointed alert floods, inevitably leading to alert fatigue and localized, reactive incident handling. By integrating the formalized resilience metrics, administrators can execute a dynamic, state-aware response strategy governed by precise mathematical thresholds rather than raw alert volumes. Specifically, this framework provides the following actionable guidelines for dynamic infrastructure management:

State A: High Exposure, Stable Capacity (Absorptive Phase):

If the Exposure metric (E_{exp}) spikes but the Absorptive Capacity index (C_{abs}) remains robust (e.g., consistently ≥ 0.8), the infrastructure is effectively diffusing the stress. This pattern is highly characteristic of intermittent scanning or low-impact distributed probing. The actionable NOC directive here is strict monitoring; administrators should intentionally delay aggressive interventions (such as blanket IP blocking) to avoid self-inflicted availability drops and disruption of legitimate user traffic.

State B: Critical Degradation Trajectory (Exhaustion Phase):

If C_{abs} continuously deteriorates and breaches a critical operational threshold (e.g., drops below 0.5) across sequential flow windows, it mathematically signals impending structural exhaustion. This metric serves as a real-time predictive trigger, moving the NOC ahead of actual service failure. The actionable response dictates immediate, automated mitigation: deploying aggressive rate-limiting policies, initiating BGP blackholing at edge routers, or dynamically provisioning redundant server instances to absorb the mathematically proven overflow.

State C: Recovery Bottlenecks (Stabilization Phase):

Following the mitigation of a disruptive event, the recovery metric (R_{rec}) actively monitors the stabilization trajectory. If the calculated decay constant (λ) of the traffic deviation flattens prematurely, it flags hidden persistence—such as secondary lateral infections or latent routing misconfigurations—hindering full system recovery. This specific insight directs operations teams to initiate targeted forensic audits rather than prematurely closing the incident ticket. By translating raw IDS logs into these quantifiable, actionable resilience states, the proposed framework empowers security teams to definitively shift from reactive alert-chasing to strategic, data-driven resilience management.

4.5. Parameter Sensitivity Analysis

The proposed framework relies on specific design parameters, primarily the anomaly density threshold (set at 5%) and the catastrophic persistence limit ($T_{max} = 20$). To ensure the robustness of the Absorptive Capacity (C_{abs})

DOI: 10.46121/pspc.54.1.18

metric, we conducted a sensitivity analysis to observe how parameter variations affect its statistical correlation with physical network degradation (NT_{deg}).

First, we varied the anomaly density threshold. Lowering the threshold to 2% made the framework overly sensitive to benign traffic spikes. This introduced operational noise and visibly reduced the Pearson correlation from 0.88 to approximately 0.76. Conversely, increasing the threshold to 10% made the detection mechanism too rigid. The system missed early-stage degradation signs, causing the correlation to drop to 0.81. The 5% threshold proved mathematically optimal for filtering background noise while capturing genuine structural stress.

Next, we adjusted the persistence limit (T_{max}). Halving T_{max} to 10 windows triggered premature exhaustion alerts. The metric signaled failure well before the actual physical throughput collapsed ($r \approx 0.72$). Extending T_{max} to 30 windows created a delayed reaction; the network often suffered severe performance drops before C_{abs} fully depleted ($r \approx 0.83$). The $T_{max} = 20$ setting aligned best with the actual structural buffering capacity of the tested infrastructure.

These findings confirm that while the framework is highly adaptable, operators must calibrate these threshold parameters against the specific historical traffic baselines of their target networks to maintain high predictive accuracy.

DISCUSSION

The findings of this study provide a rigorously validated quantitative perspective on how intrusion detection outputs can be analytically leveraged to assess cyber resilience in computer networks. Rather than treating IDS alerts and traffic-derived indicators as isolated tactical security signals, the proposed framework mathematically formalizes these routinely available outputs into continuous, state-aware resilience indicators. This perspective aligns with modern resilience paradigms that emphasize understanding systemic behavior under disruption, moving significantly beyond mere qualitative detection evaluation.

A key observation emerging from the empirical validation is that different classes of IDS-derived indicators reliably inform distinct resilience-related aspects. The analysis demonstrates that Exposure (E_{exp}) serves as a highly sensitive early-warning metric, effectively distinguishing between active attack phases and normal operations. Crucially, the fundamental shift of this framework from a conceptual mapping to a quantitatively validated assessment tool is evidenced by the Absorptive Capacity (C_{abs}). By mathematically proving the strong correlation ($|r| \approx 0.88$) between the IDS-derived C_{abs} and physical network degradation (NT_{deg}), the study establishes that these indicators serve as reliable, real-time computational proxies for structural service exhaustion. The analysis of traffic deviation and disruption duration further complements these alert-based observations. The strong correlation observed in the Recovery-Related Behavior (R_{rec}) confirms that the temporal decay of traffic deviation effectively mirrors the ground-truth recovery trajectory. The differing temporal trends observed across E_{exp}, C_{abs}, and R_{rec} demonstrate that systemic resilience cannot be captured by a single static metric; instead, it requires the continuous, multi-dimensional temporal analysis of system behavior under stress.

Importantly, while the empirical validation confirms the operational accuracy of the derived metrics, these indicators represent continuous structural states rather than static, binary security scores. By explicitly anchoring these states to actionable Network Operations Center (NOC) directives, the proposed approach mitigates the risk of alert fatigue and avoids overgeneralization. From a practical perspective, the framework offers immense value by leveraging existing intrusion detection infrastructures. It eliminates the need for additional monitoring mechanisms, specialized sensors, or complex simulation environments, seamlessly integrating operational data into automated, real-time resilience evaluation processes.

While the empirical validation confirms the framework's efficacy under high-stress conditions, we must acknowledge certain operational boundaries. The current experimental setup specifically targets volumetric DDoS attacks. These attacks aim to cause rapid structural exhaustion, which aligns perfectly with our minute-scale flow windows and high-density anomaly thresholds. However, real-world cyber resilience must also account for 'low-and-slow' campaigns, such as Advanced Persistent Threats (APTs). Unlike DDoS floods, APTs operate below typical volumetric detection thresholds, focusing on stealthy lateral movement and gradual data exfiltration.

DOI: 10.46121/pspc.54.1.18

To adapt our framework for such covert threats, the temporal parameters require significant recalibration. For instance, the sequential flow window (T) would need to shift from minutes to days or even weeks to capture the slow accumulation of anomalies. Furthermore, the severity weights (w_i) within the Exposure metric (E_{exp}) must be heavily reassigned to prioritize lateral movement signatures or privilege escalation alerts over raw traffic volume. This context-aware parameterization demonstrates the mathematical flexibility of our approach while clearly defining the scope of the current experimental findings.

Overall, the primary contribution of this study lies in successfully bridging the gap between tactical intrusion detection outputs and strategic cyber resilience quantification. By providing an assessment-oriented analytical layer that is both mathematically rigorous and practically feasible, the framework directly supports the transition of network security practices from reactive incident handling to proactive, data-driven resilience management.

CONCLUSION

This study successfully bridged the operational gap between intrusion detection capabilities and comprehensive cyber resilience evaluation. By introducing a mathematically formalized assessment framework, we demonstrated that routinely generated IDS outputs can be rigorously repurposed into quantifiable, real-time indicators of system resilience under disruptive conditions. Through empirical validation using the benchmark CSE-CIC-IDS2018 dataset, the research moved beyond qualitative mapping. The statistical linkage established between the formulated Absorptive Capacity metric and physical network throughput degradation ($r \approx 0.88$) proved that IDS alert persistence patterns are highly reliable proxies for structural service exhaustion. Furthermore, the characterization of stability and recovery dynamics (λ) showcased the framework's ability to project system restoration trajectories. From a practical standpoint, this methodology empowers Network Operations Centers (NOCs) with an actionable, data-driven decision-support layer. By translating disjointed alert floods into cohesive resilience states, administrators can execute state-aware mitigations, avoiding alert fatigue and premature incident closures. Crucially, this is achieved without imposing additional monitoring overhead or complex simulation requirements on existing infrastructures. Future research should focus on extending this mathematical formalization across diverse IDS technologies and decentralized edge-computing environments. Additionally, integrating these real-time resilience indicators into automated orchestration platforms (such as SOAR) could pave the way for self-healing network architectures driven directly by continuous traffic analytics.

REFERENCES

1. J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," Computer Networks, vol. 54, no. 8, pp. 1245–1265, 2010. https://doi.org/10.1016/j.comnet.2010.03.005
2. Z. Cao, H. Zhao, Y. Wang, C. He, D. Zhou, and X. Han, "A resilience quantitative assessment framework for cyber–physical systems: Mathematical modeling and simulation," Applied Sciences, vol. 15, no. 15, p. 8285, 2025. https://doi.org/10.3390/app15158285
3. H. Cho, J. Kim, S. Lee, and Y. Park, "Quantifying cyber resilience: A framework based on availability metrics and AUC-based normalization," Electronics, vol. 14, no. 24, p. 2465, 2025. https://doi.org/10.3390/electronics14242465
4. I. Linkov, T. Bridges, F. Creutzig, J. Decker, C. Fox-Lent, W. Kroeger, J. Lambert, A. Levermann, B. Montreuil, J. Nathwani, R. Nyer, O. Renn, B. Scharte, A. Scheffler, M. Schreurs, and T. Thiel-Clemen, "Changing the resilience paradigm," Nature Climate Change, vol. 4, no. 6, pp. 407–409, 2014. https://doi.org/10.1038/nclimate2227
5. C. G. Rieger, D. I. Gertman, and M. A. McQueen, "Resilience analysis for engineered systems," Proceedings of the IEEE, vol. 99, no. 1, pp. 1–6, 2010. https://doi.org/10.1109/JPROC.2010.2059937

DOI: 10.46121/pspc.54.1.18

6. D. D. Woods, "Four concepts for resilience and the implications for the future of resilience engineering," Reliability Engineering & System Safety, vol. 141, pp. 5–9, 2015. https://doi.org/10.1016/j.ress.2015.03.018
7. C. Nan and G. Sansavini, "A quantitative method for assessing resilience of interdependent infrastructures," Reliability Engineering & System Safety, vol. 157, pp. 35–53, 2017. https://doi.org/10.1016/j.ress.2016.08.013
8. C. Nan, G. Sansavini, and W. Kröger, "Building an integrated metric for quantifying the resilience of interdependent infrastructure systems," in Critical Information Infrastructures Security, Springer, 2016, pp. 159–171. https://doi.org/10.1007/978-3-319-31663-5_14
9. N. Hoque, M. H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya, and J. K. Kalita, "Network attacks: Taxonomy, tools and systems," Journal of Network and Computer Applications, vol. 40, pp. 307–324, 2014. https://doi.org/10.1016/j.jnca.2013.08.001
10. H. Cho, J. Kim, S. Lee, and Y. Park, "A metric selection framework for cyber resilience assessment based on ME/CE principles," Electronics, vol. 14, no. 16, p. 1684, 2025. https://doi.org/10.3390/electronics14161684
11. J. Pérez, L. Labaka, and J. Hernantes, "Cyber resilience and incident response in smart cities: A systematic literature review," Smart Cities, vol. 3, no. 3, pp. 865–898, 2020. https://doi.org/10.3390/smartcities3030046
12. [12] S. M. AlHidaifi and M. R. Asghar, "Towards a cyber resilience quantification framework (CRQF) for IT infrastructure," Computer Networks, vol. 247, p. 110446, 2024. https://doi.org/10.1016/j.comnet.2024.110446
13. A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," Cybersecurity, vol. 2, no. 1, p. 20, 2019.
14. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," Journal of Information Security and Applications, vol. 50, p. 102419, 2020.
15. S. Thakkar and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT," Archives of Computational Methods in Engineering, vol. 28, no. 4, pp. 2819–2843, 2021.
16. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), 2018, pp. 108–116.
17. C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80–84, 2017.
18. J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communication Review, vol. 34, no. 2, pp. 39–53, 2004.
19. T. Hassan, J. P. E. G. O. Martins, F. E. F. C. B. F. E. S. D. Santos, and N. F. F. D. Silva, "Alert fatigue in cybersecurity: A systematic literature review," IEEE Access, vol. 8, pp. 185017–185039, 2020.
20. A. S. Alqahtani, A. M. Alqahtani, and M. A. Al-Makhadmeh, "SOC analysts' perceptions of alert fatigue: An empirical study," Computers & Security, vol. 124, p. 102967, 2023.

DOI: 10.46121/pspc.54.1.18

21. S. K. Singh and P. K. Gupta, "Network traffic analytics using machine learning: A comprehensive review," Computer Networks, vol. 223, p. 109590, 2023.
22. Z. Chen, Y. Liu, and J. Wang, "Flow-based temporal feature extraction for anomaly detection in software-defined networks," IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 450–464, 2023.
23. A. M. Ahmed and M. S. Al-Rubaie, "Evaluating QoS degradation under heavy network traffic analytics: Models and challenges," Journal of Network and Systems Management, vol. 32, no. 1, p. 14, 2024.

DOI: 10.46121/pspc.54.1.18