Published *online* on the journal's web page : http://innovatics.unsil.ac.id

Innovation in Research of Informatics (INNOVATICS)

| ISSN (Online) 2656-8993 |

SILPA: A Secure Layered Architecture for Institutional LAN/WLAN Performance Measurement and Automated Reporting

Sutiyo[1], Hassan Rizky Putra Sailellah[2]

[1,2]Telkom University, Jl. Telekomunikasi No. 1, Terusan Buah Batu, Bandung 40257, Indonesia

[1]tioatmadja@telkomuniversity.ac.id, [2]hassanrizkyhrs@telkomuniversity.ac.id

ARTICLE INFORMATION

Article History:
Received: February 21st, 2026
Last Revision: March 9th, 2026
Published *Online*: March 28th, 2026

KEYWORDS

Active Network Measurement,
LAN/WLAN Performance,
Secure Measurement Ingestion,
Network Performance Analytics,
Layered Architecture

CORRESPONDENCE

Phone: 081548501050
E-mail: *tioatmadja@telkomuniversity.ac.id*

ABSTRACT

Institutions require secure, consistent, and standardized mechanisms to assess LAN and WLAN performance, yet existing monitoring tools often produce fragmented measurements without validation or automated reporting. This study presents the Secure Institutional Layered Performance-Assessment Architecture (SILPA), a unified framework combining active measurement, token-protected ingestion, standards-aligned analytics, and automated documentation. SILPA employs Windows-based agents, schema-validated REST ingestion, IPPM-aligned metrics, and a standardized sampling model to ensure accuracy and comparability across heterogeneous environments. A 30-day deployment across LAN and WLAN segments at Institution XYZ produced 341 validated samples from 55 evaluation units and 61 paths, with stable LAN performance (0.5 ms latency, 0.2 ms jitter) and expected WLAN variability (18.7 ms latency, 35.2 ms jitter, 0.55% loss). All records passed authentication and schema checks, and SILPA consistently generated structured A4-formatted reports. These results demonstrate that SILPA provides a reliable, secure, and reproducible approach for institutional network-performance evaluation, reducing fragmentation and enabling audited, governance-ready assessments. Future extensions will explore multi-institution deployment and predictive analytics.

1. INTRODUCTION

Institutions increasingly depend on network connectivity for daily processes. However, many organizations use fragmented monitoring tools, which produce inconsistent results and make it hard to obtain standardized, comparable, and decision-ready insights across LAN and WLAN environments. Moreover, while existing dashboards focus on visualizations over structured reporting, manual extraction, aggregation, and formatting of network data are often required, leading to variability and inefficiency [1], [2].

Modern network infrastructures generate abundant performance data, such as logs, flow records, SNMP telemetry, and active measurement probes [3]. However, when networks lack automated pipelines and analytics engines, operators often underutilize this data, highlighting the need for normalization mechanisms that convert raw measurements into decision-ready insights [4]. Furthermore, campus and enterprise networks increasingly require continuous, real-time monitoring to identify anomalies and maintain reliability. Yet, real-time visibility alone does not suffice; networks must also implement standardized processing models to ensure comparability across segments [5].

Modern networks generate abundant telemetry, but studies show this data is rarely integrated into a unified workflow. Collection, secure transmission, and analytics are often separated, reducing usefulness for decision-making [6], [7]. Research on campus wireless monitoring similarly highlights the need for processing real-time measurements to yield useful insights [8]. Surveys on layered architectures also stress the value of standard ingestion and normalization for consistency across devices and environments [6]. Contemporary work emphasizes that pipelines should transform varied measurements into actionable, audit-ready reports [9]. Taken together, these studies underscore the need for an end-to-end architecture that ensures secure, standardized,

institution-grade performance assessments. Security makes large-scale monitoring even more complex [10]. Continuous ingestion of measurement data from many clients requires strong authentication and authorization. Token-based models like OAuth 2.0/Bearer tokens enable scalable authorization, but need strict token management, origin checks, and integrity enforcement to prevent misuse [11], [12]. Meanwhile, the IETF IPPM framework [13] defines network metrics like latency, jitter, and packet loss. However, it does not specify how institutions should use these metrics in automated reporting pipelines.

To address these limitations, this study proposes a layered architecture for real-time LAN / WLAN performance measurement, integrating four main components: Windows-based data collection; secure, bearer-token-protected REST ingestion; standards-aligned analytics and scoring; and automated report generation in PDF and Word formats. This architecture Secure Institutional Layered Performance Assessment Architecture (SILPA) is implemented as a prototype. By bridging raw telemetry with formal reporting, SILPA enables a secure, interoperable workflow for network-performance governance.

This study builds on this architectural base and introduces key innovations that distinguish SILPA from previous monitoring frameworks. Unlike earlier works that examine wireless analytics, anomaly detection, layered monitoring, security mechanisms, or IP measurement standards in isolation, SILPA integrates them into a single institutional workflow. Its novelty is fourfold: (i) it combines LAN and WLAN assessment under a standardized evaluation-unit model; (ii) it embeds secure, schema-validated ingestion into the measurement pipeline; (iii) it applies standards-aligned normalization to ensure reproducibility; and (iv) it automates structured, audit-ready performance reports. No previous framework, to our knowledge, brings acquisition, secure ingestion, standard processing, and institutional reporting together in a single, governance-focused architecture.

2. RELATED WORK

Network performance monitoring has evolved over the past decade in both academic and enterprise environments. Earlier studies focused on ad hoc testing. More recent work highlights automated analytics pipelines, standardization, and secure data collection.

a. Real-Time Monitoring in Institutional Networks

Several works propose frameworks that automate wireless network measurement and convert telemetry into insights. Recent studies [3], [4], [14] demonstrate campus-scale systems that use supervised learning and web service analytics for Wi-Fi assessment. Other research emphasizes ongoing measurement to support quality-of-service planning and long-term institutional network optimization [15], [16].

b. Performance Monitoring and Network Analytics

Network performance monitoring involves tracking metrics such as bandwidth, latency, packet loss, uptime, and jitter. Recent reviews show a shift from basic monitoring to AI-driven analytics that identify patterns, anomalies, and root causes more effectively than manual tools. Modern studies cover machine-learning-based anomaly detection and predictive analytics for reliability and faster response [17], [18], [19]. NetFlow-based active measurement frameworks have scaled to large environments using hardware acceleration. These show ultra-low latency and high throughput for real-time analytics [2], [7], [20], [21].

c. Layered Architectures for Monitoring Systems

Layered architecture helps manage complexity in distributed systems. Surveys on IoT and monitoring stress modular separation among data collection, preprocessing, and analytics. This improves scalability, interoperability, and adaptability [1], [3], [5], [6], [9]. Modular design supports modern observability platforms and aligns with reporting-oriented monitoring. Integrated systems with matching hardware and software have shown better management and security in distributed settings [14], [22], [23]. SILPA's multi-layer approach separates data collection, secure ingestion, analytics, and reporting [24].

d. Security Considerations in Monitoring Pipelines

Secure ingestion is critical in large-scale monitoring. OAuth 2.0 best practices require strict token management and sender-binding for API protection. Mitigating replay attacks is also important [11]. Research from [12] shows token authentication aids auditability and integrity. Real-time systems with IDS/IPS components can stop threats before escalation [21], [25]. Security is vital throughout measurement pipelines.

e. Standardized Measurement Definitions (IPPM)

The IETF IP Performance Metrics (IPPM) framework defines latency, delay variation, and packet loss. IPPM is widely used but focuses only on metric definitions. It does not cover end-to-end reporting. Standards like RFC 8186 improve reproducibility and consistency across networks [13], [24].

f. Hierarchical and Distributed Monitoring Systems

Recent advances in distributed observability highlight on-demand monitoring at many layers. [3] propose a scalable monitoring architecture with structured data flow and multilayer coordination. This fits well with large administrative settings and aligns with SILPA's layered principles. Prior studies have advanced real-time network monitoring, WLAN analytics, performance modeling, layered design, secure telemetry, and standardized metric definitions. Yet most examine each aspect in isolation, rather than as part of a unified process. Existing frameworks typically focus on limited functions such as wireless probing, anomaly-detection pipelines, or modular IoT monitoring and present results via dashboards or summaries, not structured, audit-ready reports for governance.

Security enhancements, such as OAuth authorization, token-based access, and IDS/IPS threat detection, improve specific monitoring tools. However, these mechanisms are rarely combined with schema validation or harmonized analytical models for institutional reporting. Current systems do not reconcile LAN and WLAN measurements under a common standard, making comparison and evaluation difficult. SILPA addresses these limitations by integrating measurement, secure transmission, standards-based processing, and reporting into a single, governance-focused architecture. Table 1 details how SILPA integrates

LAN/WLAN assessment, secures validated ingestion, normalizes metrics reproducibly, and generates A4-ready documents, providing completeness and institutional readiness lacking in earlier approaches.

TABLE 1. COMPARISON BETWEEN EXISTING MONITORING AND SILPA

Category	Existing Approaches	SILPA Contribution
Monitoring & Analytics	Focus on WLAN-only probes and ML/NetFlow-based analytics; they lack a unified LAN+WLAN scope and consistent measurement units.	Integrated LAN+WLAN probing with a standardized evaluation-unit model for reproducible comparisons across diverse areas.
Architectures, Standards & Security	Modular IoT/network layers, IPPM/TWAMP metrics, and isolated OAuth/IDS security; components work independently and rarely form a full workflow.	Cohesive architecture combining secure ingestion (OAuth/Bearer, schema checks), standards-aligned normalization, and unified processing end-to-end.
Reporting & Governance	Dashboards and basic exports without structured, audit-ready documentation for governance.	Automated A4-formatted reports with validated metrics designed for institutional assessment and compliance workflows.

3. METHODOLOGY

The implemented the SILPA as an end-to-end prototype to validate the feasibility of (i) standardized, real-time measurement across LAN/WLAN segments, (ii) secure ingestion over a token-protected REST interface, (iii) normalized analytics with a reproducible health-scoring model, and (iv) automated, report-ready outputs. The evaluation focuses on the correctness and stability of the pipeline, ingestion latency, and consistency of computed scores across repeated runs across heterogeneous institutional areas (wired and wireless).

3.1 System Architecture

The overall design of the Secure Institutional Layered Performance-Assessment Architecture (SILPA) is illustrated in Figure 1, which depicts the coordinated interaction among the data-collection agents, the token-secured ingestion interface, the analytical processing pipeline, the persistence subsystem, and the reporting layer. SILPA is structured as a sequence of tightly integrated functional layers that collectively provide a unified and secure workflow for institutional network-performance assessment. Through this layered organization, the architecture supports consistent data acquisition, authenticated and validated ingestion, standards-aligned analytical processing, and structured aggregation.

Each layer helps ensure that measurement data collected across diverse LAN and WLAN environments is uniformly validated, normalized, and stored. This guarantees that raw telemetry is transformed into reliable, comparable, and governance-ready analytical outputs. In addition, the architecture is designed to maintain consistency across heterogeneous deployment areas, enabling reproducible evaluation and facilitating downstream reporting and decision-making processes.

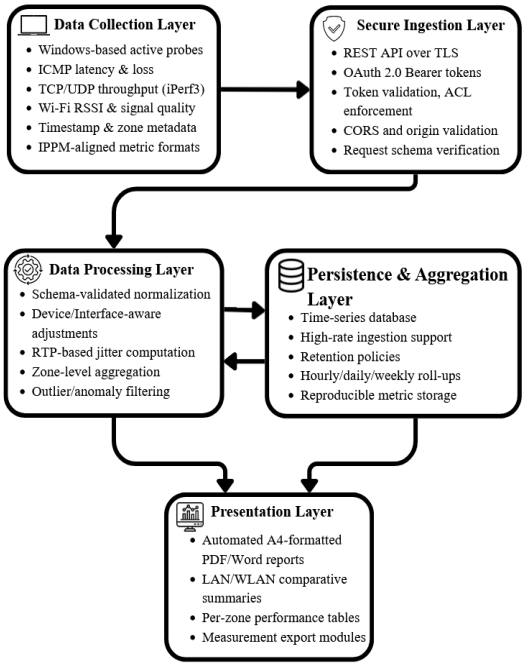

FIGURE 1. OVERVIEW OF THE SILPA LAYERED ARCHITECTURE

The SILPA framework is structured as a multi-layer architecture that integrates several interoperating components, each responsible for a distinct stage of measurement acquisition, secure ingestion, analytical processing, aggregation, and institutional reporting, as detailed below.

3.1.1 Data Collection Layer

A lightweight Windows-based data collection layer is responsible for performing continuous network measurements, including latency, throughput, jitter, packet loss, signal quality, and device status across both wired and wireless environments. The collector operates as a real-time agent that captures performance metrics using definitions aligned with the IETF IP Performance Metrics (IPPM) framework, ensuring consistency, interoperability, and reproducibility. Each measurement sample is timestamped and annotated with location or area identifiers, enabling standardized comparisons across different evaluation units or measurement locations within an institutional network.

The data collection process relies on active probing techniques executed at controlled intervals by Windows agents. These probes include ICMP ping for round-trip time and packet loss estimation, iPerf3 TCP/UDP tests for throughput and jitter analysis, and native Wi-Fi diagnostics for RSSI and link-quality assessment [26], [27]. All collected measurements are systematically tagged with temporal and spatial metadata, supporting consistent evaluation across measurement locations within higher processing layers [28], [29].

3.1.2 Secure Ingestion Layer

The ingestion layer delivers measurement data to a secure REST API that employs bearer-token authentication to regulate access. Each submission undergoes token verification, access-control checks, and CORS enforcement, ensuring that only authorized

Windows-based collectors and approved administrative dashboards can interact with the endpoint. These controls collectively maintain strict origin validation and prevent unauthorized data ingestion [10].

All measurement traffic is transmitted over TLS and protected using OAuth 2.0/Bearer tokens in accordance with the OAuth 2.0 Security Best Current Practice (RFC 9700) and the foundational authorization framework (RFC 6749), with additional provisions for native-application behavior following RFC 8252. Before acceptance, the system validates both token integrity and request-schema conformity, ensuring auditability, consistent application of security policy, and reliable protection across the entire ingestion path [11], [30], [31].

3.1.3 Data Processing Layer

The data processing layer conducts structured normalization and schema-based validation on all incoming measurements, transforming raw records into standardized performance indicators and comparative analytics outputs. This workflow ensures analytical consistency across institutional environments and supports reliable longitudinal comparisons. During processing, measurements are aggregated by evaluation unit and connectivity type, while anomaly-detection routines identify outliers, corrupted entries, or irregular patterns, ensuring that only statistically reliable samples contribute to subsequent evaluation stages [17], [18].

Once validated, the analytics service applies device- and interface-aware normalization and generates descriptive performance summaries. Jitter is computed using the RTP inter-arrival formulation to maintain alignment with established real-time media assessment practices [32]. These processes support consistent interpretation of network conditions across institutional environments.

3.1.4 Persistence & Aggregation

Processed metrics are stored in a time-series database optimized for high-volume writes and efficient range queries. Configurable retention policies manage data lifecycle, while roll-up aggregation computes hourly, daily, and weekly summaries for long-term trend analysis. A time series store supports high-rate writes and range queries with roll-ups (hourly/daily/weekly) to maintain performance and enable trend analysis with configurable.

3.1.5 Presentation Layer

The presentation layer delivers an interactive web dashboard with real-time charts, heatmaps, and drill-down capabilities. Configurable alerting rules trigger notifications via email or webhook when metrics exceed defined thresholds. Reports can be exported in CSV and PDF formats. The web dashboard provides real-time charts and drilldowns; scheduled tasks generate A4-ready PDFs and Word reports with uniform sections and tables for institutional use.

3.1.6 Optional cross-validation

When supported by the deployment environment, round-trip delay metrics can be independently verified using TWAMP. This mechanism provides timestamped two-way measurements that complement ICMP-based testing and help confirm the accuracy of observed latency and delay-variation patterns. By incorporating TWAMP into the validation workflow, the system can strengthen its assessment of end-to-end performance and achieve higher confidence in SLA-grade evaluations [22], [23], [33].

3.2 Measurement & Collection Framework

The employ standard, reproducible definitions for core metrics; each sample includes timestamps to support latency and jitter estimation.

3.2.1 Probing Pipeline

The probing pipeline is initiated by a Windows-based data collection agent that performs scheduled measurement tasks, including ICMP latency probes, iPerf3-based throughput and jitter assessments, and Wi-Fi diagnostic queries. Each generated sample is forwarded through a structured processing sequence that includes integrity checks and schema validation. All records are annotated with essential metadata such as UTC timestamp, probe type, evaluation-unit identifier, connectivity category (LAN or WLAN), and device attributes to ensure traceability and support consistent analytical interpretation.

3.2.2 Standards-Aligned Metric Definitions

The SILPA framework employs standard and reproducible definitions for all core performance metrics, ensuring analytical consistency and alignment with widely recognized measurement guidelines. Latency (RTT, ms) is computed using ICMP echo measurements, where the round-trip time is obtained by subtracting the transmission timestamp from the response timestamp, as shown in Equation (1).

$$RTT = t_{response} - t_{sent} \quad (1)$$

Its interpretation follows the one-way delay considerations recommended in ITU-T G.114 for conversational-quality assessments [34]. Packet loss is quantified as the proportion of transmitted packets that fail to reach their destination. It is computed by dividing the number of lost packets by the total number of packets sent and expressing the result as a percentage, as shown in Equation (2).

$$Loss(\%) = \frac{Packets_{lost}}{Packets_{sent}} \times 100 \quad (2)$$

The interpretation of this metric follows the semantics and performance objectives established in the ITU-T Y.1541 framework for IP-based network services [35]. Throughput is defined as the ratio of successfully transferred data to the duration of the measurement interval. This relationship is expressed in Equation (3).

$$Bandwidth = \frac{Data_{transferred}}{Time_{duration}} \quad (3)$$

The evaluation procedure adheres to the methodology specified in RFC 6349, which includes baseline RTT estimation, bottleneck bandwidth characterization, path-MTU verification, and multi-flow testing to ensure a rigorous, standards-aligned assessment of TCP and UDP performance [28]. Jitter represents the variability in packet delay and is computed as the root-mean-square deviation of individual latency samples from their mean, as expressed in Equation (4).

$$Jitter = \sqrt{\sum(\text{latency}_i - \frac{\mu)^2}{N}} \quad (4)$$

This study adopts the RTP inter-arrival jitter formulation to characterize packet-timing variation, ensuring methodological consistency with established real-time media performance assessment practices[32]. Signal quality (Wi-Fi RSSI) is derived from the received signal strength indicator (RSSI) using a linear transformation, as shown in Equation (5).

$$SignalQuality = (RSSI + 100) \times 2 \quad (5)$$

with the resulting value constrained to a 0–100% range. Client-reported RSSI measurements are used to assess coverage conditions and roaming behavior, following established WLAN design guidelines that recommend targets such as −67 dBm for real-time applications and the integration of SNR considerations where available.

3.3 SILPA Standard Sampling Model

The SILPA sampling standard establishes a consistent, industry-aligned measurement framework intended to produce statistically reliable network-performance indicators. Instead of defining requirements based on specific organizational structures or measurement locations, the model emphasizes the minimum sampling density required to produce stable, representative performance measurements.

A fundamental aspect of this standard is the requirement for at least 30 samples per evaluation unit, a threshold widely recognized in engineering measurement practice for yielding stable sample means under the Central Limit Theorem [36]. The complete set of standardized sampling parameters is summarized in Table 2, providing a unified reference for consistent SILPA deployment across diverse environments.

TABLE 2. SAMPLING STANDARD PARAMETERS

Category	Parameter	Standard for SILPA
Sampling Requirement	Minimum samples per evaluation unit	≥ 30 samples
Session Structure	LAN measurement sessions per evaluation unit	5 sessions
	WLAN measurement sessions per evaluation unit	5 sessions
Per-Session Probe Configuration	iPerf3 TCP test duration	10 seconds
	iPerf3 UDP test duration	10 seconds
	ICMP latency test	50 echo packets
Dataset Expectation	Minimum overall dataset volume	≈ 300 samples (aggregated across all evaluation units)
Measurement Window	Observation period	30-day rolling window

This minimum enhances the reliability of latency, jitter, throughput, and signal-quality estimations by reducing variance and improving the interpretability of comparative analyses [37].

3.4 Security Models

The ingestion interface employs bearer-token authentication for each registered collector and validates request origins through CORS enforcement. Tokens are periodically rotated to limit credential exposure, and any failed authentication or origin-validation attempts are logged and rejected. All submitted payloads undergo schema-level validation to prevent malformed inputs and to ensure data integrity before persistence.

To strengthen end-to-end protection, the ingestion API operates over TLS and implements OAuth 2.0 Bearer-token mechanisms, including audience binding, time-limited token issuance, and controlled token rotation. Security controls follow the OAuth 2.0 Security Best Current Practice as defined in RFC 9700, the core authorization model of RFC 6749, and native-application guidance from RFC 8252. Additional safeguards, such as redirect-flow protection, CSRF mitigation, and token-replay defenses, are enforced. When collectors connect through remote links or VPNs, deployment-hardening measures are applied in accordance with NIST SP 800-113 [11], [30], [31], [38].

3.5 Implementation Overview

The prototype system consists of five integrated components that collectively support automated network measurement, secure data ingestion, and standardized reporting. First, a Windows-based measurement agent conducts active probing using Ping, iPerf3, and Wi-Fi diagnostics to capture latency, throughput, jitter, and signal-quality metrics. Second, a REST-based ingestion interface secured with OAuth 2.0 Bearer authentication performs schema validation and enforces CORS policies to ensure the integrity and authenticity.

Third, an analytics service performs normalization, aggregation, and scoring procedures, enabling consistent interpretation of performance indicators across different evaluation units and connectivity types. Fourth, measurement records are stored in a time-series database optimized for high-volume ingestion and efficient temporal queries, supporting both short-term inspection and long-term trend analysis. Finally, the presentation layer provides automated generation of standardized A4-formatted PDF and Word reports, delivering consolidated performance summaries, tables, and visualizations suitable for institutional assessment and documentation.

3.6 Evaluation Methodology

The evaluation examines the end-to-end operation of the SILPA workflow across heterogeneous areas within a single institution, including multiple buildings and functional zones with differing LAN and WLAN conditions. The assessment covers measurement acquisition, secure data ingestion, analytics, and automated report generation to validate the correctness and stability of the entire architecture. Although the deployment is limited to one institution, the diversity of physical spaces, wired paths, and RF environments provides sufficient variation to exercise the full SILPA pipeline. The goal of this study is to validate architectural feasibility and reproducibility rather than to compare institutions; future work will extend SILPA to multi-institution deployments to evaluate broader generalizability.

Where applicable, the evaluation incorporates independent validation procedures to strengthen measurement accuracy. Access link performance is cross-checked using the throughput assessment guidelines

specified in RFC 6349 [28], while wireless coverage is examined with reference to standard WLAN site-survey expectations, including recommended RSSI and SNR targets for reliable operation (−67 dBm coverage thresholds) [39], [40]. This combined methodology ensures that the prototype is assessed under realistic operational conditions and that its outputs remain consistent, reproducible, and aligned with established network performance evaluation practices [2], [5].

4. RESULT AND DISCUSSION

This section presents the empirical dataset produced during the SILPA deployment, analyzes wired (LAN) and wireless (WLAN) performance characteristics, and provides an operational interpretation of the observed patterns. Each subsection builds on the previous one to illustrate how SILPA captures, processes, and contextualizes network conditions across diverse institutional areas. The SILPA prototype was deployed across wired (LAN) and wireless (WLAN) segments at Institution XYZ to evaluate end-to-end system performance, including real-time measurement acquisition, secure ingestion, normalization, aggregation, and automated reporting. The generated measurement report confirms that all submitted samples were successfully ingested with no authentication.

4.1 Measurement Dataset from SILPA Deployment

To contextualize the performance results, we first summarize the measurement dataset produced throughout the SILPA deployment. This provides the foundation for understanding the LAN and WLAN analyses that follow. In contrast to the SILPA Sampling Standard described in Section 3.3, which defines the minimum sampling density and probe configurations applicable to any institutional environment, the dataset in Table 3 reflects the actual measurements collected under the institution's operational conditions during the 30-day observation window.

TABLE 3. MEASUREMENT DATASET FROM SILPA DEPLOYMENT

Category	Description	Value
Total Samples Collected	Valid measurement records ingested and processed	**341**
Evaluation Units Measured	Distinct locations/interfaces producing usable measurement data	**55**
Connectivity Paths Evaluated	Combined LAN and WLAN measurement endpoints	**61**
Invalid or Rejected Samples	Schema, token, or integrity failures	**0**
Observation Window	Duration of continuous measurement	**30 days**

Table 3 consolidates the total number of valid samples, the evaluation units that produced usable data, the diversity of LAN/WLAN connectivity paths assessed, and the number of records rejected due to schema or authentication issues. These values represent the measurement output specific to the Institution XYZ deployment and should not be interpreted as standardized SILPA requirements. With the dataset characterized, the following subsection examines the performance of the wired (LAN) environment, which serves as a baseline for comparison with the more variable wireless conditions.

4.2 LAN Performance Metrics

The LAN measurements indicate a uniformly stable and reliable wired environment across Institution XYZ. The aggregated results show very low latency (0.5 ms) and minimal jitter (0.2 ms), reflecting uncongested switching paths and consistent queueing behavior across user-facing wired segments. Similarly, the TCP throughput of 255 Mbps (download) and 265 Mbps (upload), together with UDP performance of 215 Mbps (download) and 260 Mbps (upload), demonstrates that the measurement pipeline accurately captures sustained transfer rates across typical LAN access interfaces. These values are directly aligned with the summarized results presented in Table 4 and confirm that the SILPA probe execution, timestamp integrity, and normalization stages operate without introducing distortions into the observed metrics.

TABLE 4. LAN PERFORMANCE METRICS

Metric	Value
Average latency (ms)	0.5
Average jitter (ms)	0.2
TCP download (Mbps)	255
TCP upload (Mbps)	265
UDP download (Mbps)	215
UDP upload (Mbps)	260

Performance across the evaluated LAN endpoints remained consistent with Table 4, emphasizing that user-accessible wired segments exhibit stable, near-provisioned throughput under the institution's existing topology. The reliability of these measurements demonstrates that SILPA's ingestion and aggregation pipeline preserves metric fidelity and supports accurate temporal summarization for routine monitoring and institutional reporting.

Following the evaluation of the wired environment, WLAN performance was analyzed to capture RF-related variability and identify wireless-specific operational patterns. While the LAN environment exhibits highly stable behavior, wireless links are expected to show greater variability due to RF-dependent factors. Accordingly, the next subsection analyzes WLAN performance to contrast its characteristics with the wired baseline.

4.3 WLAN Performance Metrics

To assess wireless performance under varying RF conditions, the WLAN measurements collected during deployment were aggregated and summarized in Table 5, which presents key performance indicators for latency, jitter, packet loss, throughput, and signal quality.

WLAN performance across Institution XYZ exhibits substantially higher variability than in the wired environment, which is a characteristic of RF-based access networks. The aggregated WLAN results indicate an average latency of 18.7 ms, jitter of 35.2 ms, and packet loss of 0.55%, reflecting the combined effects of channel contention, multipath propagation, physical obstructions, and fluctuating client density. Throughput measurements show 62 Mbps TCP download, 41 Mbps TCP upload, 39 Mbps UDP download, and 78 Mbps UDP upload, with a mean signal-quality estimate of approximately 84%, corresponding to RSSI values typically ranging from –58 dBm to –65 dBm. These values are summarized in Table 5, which consolidates the WLAN performance indicators derived from the measurement dataset.

The observed WLAN metrics reflect mixed-quality wireless performance across the institution's buildings,

influenced by access-point placement, environmental geometry, and interference from adjacent RF sources.

TABLE 5. WLAN PERFORMANCE METRICS

Metric	Value
Average latency (ms)	18.7
Average jitter (ms)	35.2
Packet loss (%)	0.55
TCP download (Mbps)	62
TCP upload (Mbps)	41
UDP download (Mbps)	39
UDP upload (Mbps)	78
Signal quality (%)	84

The SILPA's evaluation-unit-based aggregation makes these spatial variations explicit, allowing network administrators to pinpoint operational constraints such as marginal coverage, AP oversubscription, or excessive jitter at room-level granularity. The consistency of these patterns with the measurement pipeline demonstrates the reliability of the SILPA normalization and validation stages in capturing WLAN behavior across diverse deployment conditions.

Beyond numerical differences, understanding the operational significance of these patterns requires interpreting how SILPA captures spatial and segment-level behavior across institutional environments. The next subsection offers this interpretation.

4.4 Operational Interpretation

The empirical results obtained from Institution XYZ reveal several important operational characteristics of the SILPA architecture and the network segments under evaluation. The measurements clearly distinguish the behavior of wired and wireless environments, demonstrating SILPA's ability to capture performance variations driven by underlying architectural differences. The wired segment consistently exhibited sub-millisecond latency (0.5 ms) and very low jitter (0.2 ms), reflecting stable switching paths and minimal queueing.

In contrast, the wireless segment showed greater variability, with an average latency of 18.7 ms, jitter of 35.2 ms, and packet-loss values around 0.55%, which are consistent with RF-dependent factors such as interference, propagation conditions, and changes in client activity. These distinctions confirm that SILPA's collection and processing pipeline accurately represents the inherent behavior of distinct network media.

The results further confirm that SILPA maintains the fidelity of the underlying measurement instruments. ICMP-based latency and packet-loss statistics remained stable across repeated measurements, while TCP and UDP throughput values exhibited expected protocol-specific behavior across both wired and wireless paths. Similarly, variations in Wi-Fi signal-quality metrics closely aligned with the observed performance differences, indicating consistent accuracy in the reporting of RF conditions. The convergence of these independent indicators validates the reliability of SILPA's schema-driven validation, timestamp integrity, and normalization routines.

In addition to validating measurement fidelity, SILPA enables the identification of operational conditions that influence performance. Wireless measurements highlighted areas with limited coverage (low RSSI values), elevated jitter, or reduced throughput characteristics commonly attributed to suboptimal access-point placement, physical obstructions, or channel congestion. Conversely, wireless areas with strong received-signal characteristics consistently delivered higher throughput and lower delay variation, indicating effective radio-frequency design and balanced channel utilization. These observations demonstrate SILPA's capability to support targeted performance analysis and inform infrastructure optimization decisions without relying on predetermined spatial segmentation.

Collectively, the operational interpretation confirms that SILPA accurately and consistently captures the performance characteristics of heterogeneous network environments. The architecture not only differentiates between wired and wireless behaviors but also reveals performance-affecting conditions within the measurement environment, supporting evidence-based network planning, troubleshooting, and continuous optimization.

These observations highlight that SILPA does more than collect raw measurements; it contextualizes them at evaluation-unit granularity, revealing spatial and segment-level performance patterns that traditional dashboard-centric tools often overlook. By integrating standardized analytics, secure ingestion, and location-aware aggregation, SILPA enables administrators to distinguish between structural conditions (e.g., stable wired throughput) and RF-dependent constraints (e.g., coverage gaps, jitter spikes, AP oversubscription). This interpretive capability directly supports targeted troubleshooting, infrastructure planning, and policy-driven network governance, demonstrating SILPA's value as an institutional-scale assessment framework.

4.5 Summary

The results from both LAN and WLAN analyses, along with their operational interpretation, can be consolidated into several key insights that reflect SILPA's effectiveness as an institutional monitoring framework. The empirical results obtained from Institution XYZ demonstrate that the SILPA architecture operates reliably and consistently across heterogeneous network environments. Throughout the deployment, SILPA consistently captured all relevant LAN and WLAN performance indicators, including latency, jitter, packet loss, throughput, and signal quality, and the secure ingestion layer processed all incoming records without authentication or schema-validation failures. The wired network exhibited highly stable behavior, with latency and jitter averaging approximately 0.5 ms and 0.2 ms, respectively, and throughput measurements aligning with expected access-layer performance.

In contrast, the wireless environment displayed broader performance variability, as evidenced by higher latency, increased jitter, moderate packet loss, and fluctuating TCP/UDP throughput. These characteristics reflect realistic RF-driven conditions influenced by physical obstructions, interference, and client distribution. SILPA's normalization and validation processes effectively captured these variations, enabling accurate representation of wireless network behavior and supporting detailed comparative analysis between wired and wireless segments.

Furthermore, SILPA's automated reporting layer consistently produced structured A4-formatted documents that consolidated measurement summaries, performance tables, and analytical visualizations. This automation highlights SILPA's capability to transform raw measurements into standardized, institution-ready outputs with minimal administrative intervention. Overall, the results confirm that SILPA provides a dependable, secure, and reproducible foundation for institutional network-performance assessment and supports advanced operational insight across diverse network conditions. Overall, these findings confirm that SILPA not only characterizes performance accurately but also provides actionable insights essential for institutional decision-making and long-term network optimization.

5. CONCLUSIONS

The deployment of SILPA at Institution XYZ demonstrates the practicality and robustness of a layered, standards-aligned architecture for institutional network-performance assessment. SILPA reliably captured all core performance indicators: latency, jitter, packet loss, throughput, and signal quality through its Windows-based active measurement agents, while the secure ingestion layer successfully validated every submitted record without authentication or schema-level failures. These outcomes confirm the correctness and stability of SILPA's end-to-end workflow across acquisition, secure ingestion, analytics, aggregation, and automated reporting.

Quantitatively, the wired environment exhibited highly stable behavior, with average latency around 0.5 ms and jitter near 0.2 ms, reflecting uncongested switching paths and consistent queueing conditions. By contrast, the wireless environment showed expected RF-driven variability, including approximately 18.7 ms latency, 35.2 ms jitter, and 0.55% packet loss, along with moderate fluctuations in TCP/UDP throughput. These differences confirm that SILPA preserves the fidelity of underlying measurement instruments and accurately differentiates performance across network media. Moreover, SILPA's evaluation-unit-based aggregation revealed localized WLAN conditions such as reduced signal quality or interference-affected areas demonstrating the system's ability not only to measure but also to contextualize network behavior at room- and segment-level granularity.

Although the evaluation was conducted at a single institution, the diversity of monitored buildings, LAN paths, and WLAN environments provides sufficiently heterogeneous conditions to validate SILPA's architectural feasibility and workflow reproducibility. The objective of this study is to demonstrate SILPA's functional correctness rather than to perform cross-institution benchmarking; nonetheless, expanding SILPA deployments across multiple institutions will be an important future direction to strengthen generalizability.

In summary, SILPA offers a secure, scalable, and reproducible foundation for institutional network-performance evaluation. By unifying standards-aligned measurement, token-secured ingestion, structured analytics, and automated reporting, SILPA advances beyond existing monitoring approaches and supports evidence-based governance in campus and enterprise environments. Future research will explore multi-institution deployments, long-term trend analysis, anomaly-detection integration, and predictive modeling to further strengthen SILPA as a comprehensive performance-management framework.

REFERENCES

[1] S. Juneja, Arshdeep, S. Maiti, S. Raweri, B. S. Bhati, and H. Sharma, "Comprehensive Evaluation of Network Performance Monitoring Solutions," in *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, IEEE, May 2024, pp. 1–6. doi: 10.1109/ISCS61804.2024.10581356.

[2] O. Khattach, O. Moussaoui, and M. Hassine, "End-to-End Architecture for Real-Time IoT Analytics and Predictive Maintenance Using Stream Processing and ML Pipelines," *Sensors*, vol. 25, no. 9, p. 2945, 2025, doi: 10.3390/s25092945.

[3] H. Madhukumar, T. A. Bower, X. Vasilakos, J. P. Ullauri, M. Lema, and D. Simeonidou, "A Scalable and Distributed Hierarchical Architecture for Network Monitoring-on-Demand," in *2024 3rd International Conference on 6G Networking (6GNet)*, 2024, pp. 63–68. doi: 10.1109/6GNet63182.2024.10765622.

[4] S. Manas Kala *et al.*, "Architecture, Performance, and Usability of Mobile Cellular Network Monitoring Applications for Data-Driven Analysis," *IEEE Access*, vol. 12, pp. 88426–88444, 2024, doi: 10.1109/ACCESS.2024.3412752.

[5] N. Yaseen, "From Counters to Telemetry: A Survey of Programmable Network-Wide Monitoring," *Network*, vol. 5, no. 3, p. 38, 2025, doi: 10.3390/network5030038.

[6] A. Raj and S. D. Shetty, "IoT Eco-system, Layered Architectures, Security and Advancing Technologies: A Comprehensive Survey," *Wirel. Pers. Commun.*, vol. 122, no. 2, pp. 1481–1517, Jan. 2022, doi: 10.1007/s11277-021-08958-3.

[7] Z. Long and W. Jinsong, "Network Traffic Classification Based on a Deep Learning Approach Using NetFlow Data," *Comput. J.*, vol. 66, no. 8, pp. 1882–1892, 2023, doi: 10.1093/comjnl/bxac049.

[8] Q. and C. J. and F. Z. and H. Long Tingting and Guo, "Automatic Analysis Framework for Campus Wireless Network Performance Based on Web Services and Supervised Learning Methods," in *Computer Applications*, C. and H. L. and J. W. and C. X. and S. X. and L. Z. Yu Haipeng and Cai, Ed., Singapore: Springer Nature Singapore, 2024, pp. 14–33.

[9] J. Tian Yu-Chu and Gao, "Network Performance Architecture," in *Network Analysis and Architecture*, Singapore: Springer Nature Singapore, 2024, pp. 275–320. doi: 10.1007/978-981-99-5648-7_8.

[10] D. Soldani *et al.*, "eBPF: A New Approach to Cloud-Native Observability, Networking and Security for Current (5G) and Future Mobile Networks (6G and Beyond)," *IEEE Access*, vol. 11, pp. 57174–57202, 2023, doi: 10.1109/ACCESS.2023.3281480.

[11] T. Lodderstedt, J. Bradley, A. Labunets, and D. Fett, "Best Current Practice for OAuth 2.0 Security," Jan. 2025, *RFC Editor*. doi: 10.17487/RFC9700.

[12] P. Rujichaikul and I. Rassameeroj, "Token-Based Authentication Monitoring System," *Journal of Cyber Security and Mobility*, Oct. 2025, doi: 10.13052/jcsm2245-1439.1441.

[13] G. Mirsky and I. Meilik, "Support of the IEEE 1588 Timestamp Format in a Two-Way Active Measurement Protocol (TWAMP)," Jun. 2017, *RFC Editor*. doi: 10.17487/RFC8186.

[14] J. A. Marques and L. P. Gaspary, "Advancing Network Monitoring and Operation with In-band Network Telemetry and Data Plane Programmability," in *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, IEEE, May 2023, pp. 1–6. doi: 10.1109/NOMS56928.2023.10154387.

[15] F. Wilhelmi, S. Szott, K. Kosek-Szott, and B. Bellalta, "Machine Learning & Wi-Fi: Unveiling the Path Towards AI/ML-Native IEEE 802.11 Networks," 2024. doi: https://doi.org/10.48550/arXiv.2405.11504.

[16] B. Liu, K. Zhao, L. Huang, and H. Xu, "Wireless Performance Test and Evaluation for New Generation Wi-Fi Router," in *2024 Photonics & Electromagnetics Research Symposium (PIERS)*, IEEE, Apr. 2024, pp. 1–7. doi: 10.1109/PIERS62282.2024.10618773.

[17] S. Schmidl, P. Wenig, and T. Papenbrock, "Anomaly Detection in Time Series: A Comprehensive Evaluation," *Proceedings of the VLDB Endowment*, vol. 15, no. 9, pp. 1779–1797, 2022, doi: 10.14778/3538598.3538602.

[18] Z. Li *et al.*, "Situation-Aware Multivariate Time Series Anomaly Detection Through Active Learning and Contrast VAE-Based Models in Large Distributed Systems," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 9, pp. 2746–2765, Sep. 2022, doi: 10.1109/JSAC.2022.3191341.

[19] S. Szott *et al.*, "Wi-Fi Meets ML: A Survey on Improving IEEE 802.11 Performance with Machine Learning," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1843–1893, 2022, doi: 10.1109/COMST.2022.3179242.

[20] K. Jaswanth, S. Sruthi, P. Ramachandrula, and S. Saravanan, "Real-Time Network Monitoring: A Big Data Approach," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, IEEE, Jul. 2023, pp. 1–5. doi: 10.1109/ICCCNT56998.2023.10307890.

[21] Y. Chen, S. Layeghy, L. D. Manocchio, and M. Portmann, "P4-NIDS: High-Performance Network Monitoring and Intrusion Detection in P4," in *Intelligent Computing (CompCom 2025)*, vol. 1426, in Lecture Notes in Networks and Systems, vol. 1426. , Springer, 2025, pp. 355–373. doi: 10.1007/978-3-031-92611-2_24.

[22] Z. Xu, Z. Lu, and Z. Zhu, "Information-Sensitive In-Band Network Telemetry in P4-Based Programmable Data Plane," *IEEE/ACM Transactions on Networking*, vol. 32, no. 6, pp. 5081–5096, Dec. 2024, doi: 10.1109/TNET.2024.3448244.

[23] Y. Jin *et al.*, "Scheduling In-Band Network Telemetry with Convergence-Preserving Federated Learning," *IEEE/ACM Transactions on Networking*, 2023, [Online]. Available: https://ljiao.github.io/papers/ton23-intfl.pdf

[24] C. L. Aldea, R. Bocu, and R. N. Solca, "Real-Time Monitoring and Management of Hardware and Software Resources in Heterogeneous Computer Networks through an Integrated System Architecture," *Symmetry (Basel).*, vol. 15, no. 6, p. 1134, May 2023, doi: 10.3390/sym15061134.

[25] K. Papadopoulos, P. Papadimitriou, and C. Papagianni, "Deterministic and Probabilistic P4-Enabled Lightweight In-Band Network Telemetry," *IEEE Transactions on Network and Service Management*, vol. 20, no. 4, pp. 4909–4923, 2023, doi: 10.1109/TNSM.2023.3301839.

[26] B. M. Zieliński, "Assessment of iPerf as a Tool for LAN Throughput Prediction," *International Journal of Electronics and Telecommunication*, 2023, [Online]. Available: https://www.ijet.pl/index.php/ijet/article/view/10.24425-ijet.2023.146501

[27] J. Wang, G. Huang, and Z. Shao, "Performance Evaluation of Wi-Fi 6 and Technology Prospects of Wi-Fi," in *2022 International Conference on Information Processing and Network Provisioning (ICIPNP)*, IEEE, Sep. 2022, pp. 91–95. doi: 10.1109/ICIPNP57450.2022.00026.

[28] B. Constantine, G. Forget, R. Geib, and R. Schrage, "Framework for TCP Throughput Testing," Aug. 2011. doi: 10.17487/RFC6349.

[29] "iPerf3 User Documentation & man iperf3 — perform network throughput tests," Feb. 2026.

[30] M. B. Jones and D. Hardt, "The OAuth 2.0 Authorization Framework: Bearer Token Usage," Oct. 2012, *RFC Editor*. doi: 10.17487/RFC6750.

[31] W. Denniss and J. Bradley, "OAuth 2.0 for Native Apps," Oct. 2017. doi: 10.17487/RFC8252.

[32] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications," Jul. 2003. doi: 10.17487/RFC3550.

[33] K. Hedayat, R. Krzanowski, A. Morton, K. K. Yum, and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," Internet Engineering Task Force (IETF).

[34] "One-way Transmission Time," Geneva, Switzerland, May 2003.

[35] "Network Performance Objectives for IP-based Services," Geneva, Switzerland, Dec. 2011.

[36] Rubiktop, "The Magic Number 30: Why a Sample Size of 30 Is Often Considered Sufficient for Statistical Significance," 2023. [Online]. Available: https://www.linkedin.com/pulse/magic-number-30-why-sample-size-often-considered-sufficient

[37] A. A. Hassoon Almelli and M. S. N. Almhanna, "Comprehensive Analysis of Network Performance Using Various Metrics and Algorithms," *Journal of Information Systems Engineering and Management*, vol. 10, no. 11s, pp. 1–15, 2025, [Online]. Available: https://www.jisem-journal.com/index.php/journal/article/download/1630/631/2649

[38] S. Frankel, P. Hoffman, A. Orebaugh, and R. Park, "NIST Special Publication 800-113: Guide to SSL VPNs," Jul. 2008.

[39] Cisco Systems, "Understand Site Survey Guidelines for WLAN Deployment," Nov. 2023.

[40] Cisco Meraki, "Signal-to-Noise Ratio (SNR) and Wireless Signal Strength," May 2025.

AUTHORS

Sutiyo

He is a lecturer at the School of Computing, Telkom University, focusing on computer networks, wireless networking, and cloud computing. His work spans both teaching and research in modern network technologies.

Hassan Rizky Putra Sailellah

He is a lecturer at the School of Computing, Telkom University. He earned his master's degree in computer science from Telkom University in 2024. His work focuses on artificial intelligence, machine learning, deep learning, and the IoT.