Techno Nusa Mandiri: Journal of Computing and Information Technology
Vol. 23, No. 2 September 2026 | DOI https://doi.org/10.33480/techno.v23i2.8695

DESIGN AND DEPLOYMENT OF ISOLATION FOREST AIOPS FOR AVAYA INFRASTRUCTURE ANOMALY DETECTION

Wan Berry Pranata[1*]; Eni Heni Hermaliani[2]; Rizqia Fauziah[3]; Joharini[4]; Windu Gata[5]

Faculty of Information Technology[1,2,3,4,5]
Universitas Nusa Mandiri, Jakarta, Indonesia[1,2,3,4,5]
http://www.nusamandiri.ac.id[1,2,3,4,5]
14250031@nusamandiri.ac.id[1*], enie_h@nusamandiri.ac.id[2], 14250029@nusamandiri.ac.id[3],
14250002@nusamandiri.ac.id[4], windu@nusamandiri.ac.id[5]

(*) Corresponding Author



The creation is distributed under the Creative Commons Attribution-NonCommercial 4.0 International License.

Abstract—*Unified Communication (UC) infrastructure such as the Avaya Telephony ecosystem is highly critical and demands high availability. Traditional monitoring systems generally rely on static thresholds that often fail to detect distributed systemic anomalies before fatal failures occur. This study proposes an Artificial Intelligence for IT Operations (AIOps) system design in the form of a modular software pipeline for multivariate anomaly detection based on time-series data. Experiments were conducted using a real dataset of 118,738 rows of monitoring metrics logs of critical Avaya components, including Session Border Controller (SBC), Session Manager (SM), Communication Manager (CM), Avaya Media Server (AMS), and Avaya Aura Device Services (AADS). The Isolation Forest algorithm was applied unsupervised to extract distributed cross-host anomaly patterns. The results showed that the model successfully identified 5,937 systemic anomalies from the total operational data (5% contamination rate). Software performance testing demonstrated high computational efficiency with very fast inference times, making it highly suitable for integration as a proactive monitoring module. The contribution of this research lies in the integration of monitoring software engineering architecture with artificial intelligence for automation of telecommunications infrastructure management.*

Keywords: *AIOps, Avaya Telephony, Anomaly Detection, Isolation Forest, Zabbix Monitoring.*

Intisari—Infrastruktur Unified Communication (UC) Enterprise seperti ekosistem Avaya Telephony bersifat sangat kritis dan menuntut ketersediaan tingkat tinggi (high availability). Sistem pemantauan tradisional umumnya mengandalkan ambang batas (threshold) statis yang sering kali gagal mendeteksi anomali sistemik terdistribusi sebelum kegagalan fatal terjadi. Penelitian ini mengusulkan sebuah rancang bangun sistem Artificial Intelligence for IT Operations (AIOps) berupa pipeline perangkat lunak modular untuk deteksi anomali multivariat berbasis data runtun waktu (time-series). Eksperimen dilakukan menggunakan dataset riil sebanyak 118.738 baris log metrik pemantauan komponen kritis Avaya, meliputi Session Border Controller (SBC), Session Manager (SM), Communication Manager (CM), Avaya Media Server (AMS), dan Avaya Aura Device Services (AADS). Algoritma Isolation Forest diterapkan secara unsupervised untuk mengekstraksi konspirasi anomali lintas host. Hasil penelitian menunjukkan model berhasil mengidentifikasi 5.937 anomali sistemik dari total data operasional (tingkat kontaminasi 5%). Pengujian performa perangkat lunak menunjukkan efisiensi komputasi yang tinggi dengan waktu inferensi yang sangat cepat, menjadikannya sangat layak diintegrasikan sebagai modul pemantauan proaktif. Kontribusi penelitian ini terletak pada integrasi arsitektur rekayasa perangkat lunak monitoring dengan kecerdasan buatan untuk otomatisasi manajemen infrastruktur telekomunikasi.

Kata Kunci: *AIOps, Avaya Telephony, Deteksi Anomali, Isolation Forest, Zabbix Monitoring.*

INTRODUCTION

Unified Communication (UC) infrastructure based on the Avaya Telephony architecture plays a crucial role as the foundation of global business operations (Tauhid & Taufiqurrrohman, 2024). The complexity of this ecosystem is formed from the integration of various specialized server components, including the Session Border Controller (SBC) for SIP session perimeter protection, Session Manager (SM) and Communication Manager (CM) as the main call

routing control engines, as well as Avaya Aura Device Services (AADS) and Avaya Media Server (AMS) which function to manage endpoint provisioning and voice media transcoding processing (Yanuar Ishaq, 2023). The characteristics of very tight interconnection between nodes imply a high vulnerability of the system to the domino effect; a small disruption to one element has the potential to paralyze the entire corporate communication path in aggregate (Lianda, 2024). To mitigate the risk of performance degradation, systems engineers commonly adopt open telemetry monitoring platforms such as Zabbix to periodically collect vital hardware parameters and network functionality (Sulasno & Saleh, 2020). By deploying monitoring agents, temporally sequential data such as processor workload, random memory space availability, ICMP response latency, and Ethernet bit rate are continuously collected (Hendra Supendar, 2025). However, this conventional monitoring mechanism has a fundamental weakness in the form of absolute reliance on static threshold-based rules (Sulasno & Saleh, 2020)

This method not only fails to adapt to non-linear daily operational load fluctuations, but also lacks the capability to recognize distributed systemic anomalies a subtle abnormality where performance indicators from multiple machines shift simultaneously without any single metric crossing an individual alarm critical limit (Siti Aisyah Aliyah & Yulindon Yulindon, 2026). Addressing these operational limitations, the modern software engineering paradigm is now transitioning towards the integration of artificial intelligence in IT operational management, or what is known as AIOps (Rahma, Indriyani, Alfian, & Sandi, 2023). This research aims to address the gap in enterprise telecommunications monitoring technology by designing an intelligent software pipeline architecture based on multivariate time series data drawn from the Zabbix (Kostopoulos, 2025). Within this system, an unsupervised machine learning algorithm in the form of Isolation Forest is embedded to independently extract operational stress patterns (Rifai & Wulandari, 2025) This engineering implementation not only automates distributed outlier detection, but also presents analytical visualizations that make it easier for operational teams to handle problems proactively before system malfunctions occur that impact the company's financial losses (Evan, A.P & Ricardo B.P, 2024).

From this research, the author raises several studies as references in enriching the study material. The following study on the optimization and automation of network infrastructure monitoring systems based on open source code has been widely explored in the latest scientific literature. (Tauhid & Taufiqurrrohman, 2024) explained the efficiency of utilizing the Zabbix architecture in providing flexible openness of distributed computing system performance information. Efforts to accelerate the delivery of monitoring alarms through the integration of real-time messaging engines based on Telegram bots have also been proven to reduce the Mean Time to Repair (MTTR) metric in handling IT infrastructure incidents (Dwiputra et al., 2025) (Wazaumi et al., 2025). Furthermore, research pioneered by (Sulasno & Saleh, 2020), (Evan, A.P & Ricardo B.P, 2024) emphasized that the dynamic use of the Zabbix Webhook feature provides high reliability for administrators in tracking memory and storage space utilization before reaching the critical phase of device failure.

However, the use of conventional systems often results in a pile of false alarms (alert fatigue) due to the inability of static algorithms to recognize the seasonal nature of server workloads (Wijanarko & Adhisa, 2023). To resolve this issue, the use of advanced analysis techniques using the Machine Learning paradigm has begun to be applied as an intelligent inference engine to complement monitoring databases. Analytical investigations by previous researchers have proven that artificial intelligence-based outlier detection is capable of objectively identifying hidden anomalies in message log structures and numerical performance metrics (Subuhanto & Tanti, 2024). Experiments in the design of this AIOps system are focused on applying a state-of-the-art multivariate detection approach to an Avaya enterprise telecommunications-specific cluster that has not been documented in previous studies.

Avaya Telephony Enterprise Ecosystem

Is an integrated IP-based voice communications (VoIP) architecture that serves massive SIP protocol signaling. Its main components (SBC, SM, CM, AADS, AMS) interact synchronously and produce multivariate performance telemetry that is highly interdependent. The Avaya Session Border Controller is a flexible, fit for purpose solution for Enterprises - that includes a set of standard security features. The Avaya Session Border Controller for Enterprise provides all the functionality required for an enterprise to terminate SIP trunks without the complexity and higher price associated with typical SBCs and scales up to 2,000 simultaneous sessions per server.

(Arcot Siva Venkates, 2025) Avaya Aura® Session Manager is the core of Avaya's revolutionary Session Initiated Protocol (SIP) based architecture. The Session Manager platform makes it possible to unify media, modes, networks, devices, applications and real-time, actionable presence across a common infrastructure, creating the web-style on-demand

access to services and applications that users increasingly expect from their enterprise communications solution.

Avaya Aura® Communication Manager software is the open, highly-reliable and extensible IP Telephony foundation on which Avaya delivers Unified Communications solutions to enterprises large and small. It delivers rich voice and video capabilities and provides for a resilient, distributed network of gateways and analog, digital and IP-based communication devices. It includes advanced mobility features, built-in conference calling and contact center applications, and E911 capabilities. Avaya Aura® Device Services provides a new set of services for Avaya's next generation of clients. These services include (Arcot Siva Venkates, 2025):

1. Enterprise login, users can log on to their Avaya device using their Enterprise credential and receive all of the Avaya Aura services they are entitled to.
2. Dynamic Configuration Service, this new configuration service dynamically generates the set of configuration parameters necessary to enable automatic bootstrapping of Avaya soft clients by searching the various Avaya databases, where configuration information is stored, and extracting and presenting relevant information to the Avaya devices.
3. Contact Service, this new service simplifies the client experience and provides a standard way of managing, storing and searching users and the enterprise contacts detail, including picture, and making them available across all of the user's devices.
4. Web Deployment Service, this service brings mobile phone deployment services to Microsoft Windows and Apple Mac OS environments. When a new device update is available within the customer's environment the user is automatically prompted to retrieve this update.

The Avaya Aura® Media Server delivers advanced multimedia processing features to a broad range of products and applications. Utilizing the latest open standards for media control and media processing, the highly scalable software-based solution deploys on standard server hardware, running Linux or Windows operating systems.

Zabbix Time Series Telemetry

An enterprise-grade monitoring tool that extracts performance data from system agents, stores it in a structured time series format, and has the ability to export data via an integrated protocol (Gevindo & Hendrik, 2025). When deployed within extensive computer network infrastructures, the systematic extraction of these multivariate metric records forms the foundational telemetry layer required to build real-time cyber resilience and operational security. By training machine learning frameworks on dense historical logs, the monitoring pipeline transforms raw data traffic into an intelligent detection system capable of identifying sophisticated intrusion footprints and distributed network anomalies at an early stage (Sari, Faiz, & Muhammad, 2025).

Continuous streaming capability ensures that critical performance indicators are constantly evaluated, shifting the maintenance paradigm from reactive troubleshooting to immediate, automated event classification. However, complex multi-source communication systems often produce highly fluctuating time-series data, making individual statistical metrics prone to elevated false-positive alarm rates (Saputra, Heri Irawan, & Mahdiyah, 2024). Integrating the structured data outputs from Zabbix nodes into an unsupervised Isolation Forest cluster minimizes computational overhead while optimizing the feature selection process.

Mathematics of the Isolation Forest Algorithm

This method is fundamentally different from clustering-based techniques or data density estimation. This algorithm isolates outlier data samples explicitly using a random binary tree structure (Isolation Trees). Mathematically, the anomaly score s(x, n) from a data sample xis calculated using the formula:

$$s(x,n) = 2^{-\frac{E(h(x))}{c(n)}} \quad (1)$$

Where E(h(x)) represents the average depth of the data path in a set of decision trees, while c(n) represents the average path length of a random search binary tree with a total of data samples ofn. Data samples that have scores close to 1 are absolutely identified as anomalies because their feature structure makes them isolated very close to the root of the decision tree (Ragil Saputro & Atina, 2025)

Research Stages

The execution flow of this intelligent software engineering research is divided into five comprehensive linear stages (Sesiati & Febrian, 2025):

1. Data Extraction, downloading 118,738 rows of historical dataset telemetry from Zabbix monitoring database repository.
2. Temporal Ingestion & Alignment, performs time index alignment to unify multivariate log files across separate servers.
3. Statistical Normalization, transforming heterogeneous ranges of performance metric values using standard statistical scaling approaches.

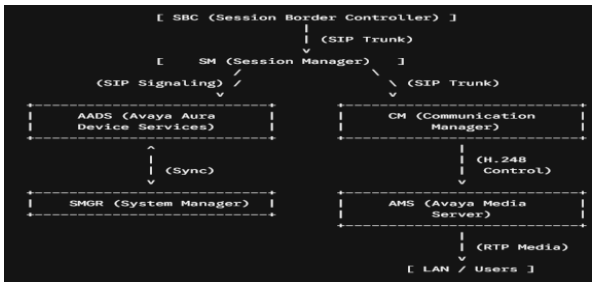
4. Machine Learning Inference, executing the Isolation Forest model in a way unsupervised with contamination parameter adjustment operational.
5. Analytical Breakdown, dissecting the most extreme moments of system failure and compiling visual documentation of technical reports.

MATERIALS AND METHODS

The proposed intelligent monitoring software architecture is built using a modular pipeline workflow approach to ensure efficient data processing and integration with real production systems (Zahratul Wahida, Data, & Amron, 2025). The figure below illustrates the logic flow from monitoring telemetry processing to generating anomaly detection inference decisions:

Avaya Aura Core Component Topology in a Data Center Environment

This section describes the architecture and internal topology of Avaya Aura core components implemented in a company's Data Center (DC) environment. This design focuses on functional relationships and protocol interconnections between key servers without involving external perimeter components such as firewalls or public networks. This system architecture uses a centralized Session Initiation Protocol (SIP) approach, where the Session Manager (SM) acts as the primary routing hub (routing core).



Source: (Research Results, 2026)

Figure 1. Avaya Topology in a Data Center

Based on Figure 1, each component within the Data Center has a specific, integrated role, as follows:

1. Session Border Controller (SBC), acts as an internal security gateway and the primary entry point for controlling and filtering VoIP (SIP) data traffic before it is forwarded to the core network within the Data Center.
2. Session Manager (SM), the core of the Session Manager architecture, functioning as a SIP proxy and primary routing agent. The SM routes all call requests (signaling) from user terminals to the appropriate feature server.
3. Communication Manager (CM), serves as the primary feature server, processing call logic, managing extension numbers (numbering plans), and providing enterprise-class telephony features. The connection between the SM and CM is established using a SIP Trunk.
4. Avaya Media Server (AMS), acts as a voice media processor (Digital Signal Processor). The AMS is directly controlled by the CM using the H.248 Gateway Control Protocol. Meanwhile, the actual voice data stream (Real-time Transport Protocol / RTP) will be streamed directly from the AMS to the user's local area network (LAN).
5. System Manager (SMGR) and Avaya Aura Device Services (AADS), SMGR acts as a centralized administration console for configuring all core elements. User data in SMGR is synchronized to AADS to provide device utilities, such as automatic configuration files and a corporate contact directory, to user terminals (end-points).

Multivariate Data Ingestion Architecture

The system receives raw input in the form of performance log files originating from five Avaya core servers (SBC, SM, CM, AMS, AADS) monitored by the Zabbix infrastructure. The extracted numerical features include processor utilization percentage (CPU Utilization), remaining physical memory capacity (Available Memory), time response package ICMP (ICMP Response Time), as well as the throughput volume of the Ethernet interface (Bit Sent/Received). The cumulative data volume used in this study covers 118,738 rows of serial data time server operations.

Table 1. Input Telemetry Features Extracted from Zabbix Platform

Server Host Component	Zabbix Telemetry Metric Key	Data Type	Feature Description & Scale
SBC (Session Border)	net.if.in[eth0], net.if.out[eth0]	Continuous	Network throughput (Bits Received/Sent)
SM (Session Manager)	icmppingsec, system.cpu.util	Continuous	ICMP response latency (s) & CPU workload (%)
CM (Comm. Manager)	net.if.out[eth1], system.cpu.util	Continuous	Signaling interface throughput & CPU load (%)
AADS (Device Services)	net.if.out[eth0], system.cpu.util	Continuous	Provisioning egress bandwidth & CPU load (%)
AMS (Media Server)	vm.memory, size [available]	Continuous	Available physical RAM capacity (Bytes)

Source: (Research Results, 2026)

Feature Preprocessing: To maintain reproducibility, raw time-series metrics extracted via Zabbix API were normalized using StandardScore (Z-score) transformation ($z = \frac{x-\mu}{\sigma}$). No dimensionality reduction (such as PCA) was applied, preserving the full multi-dimensional physical telemetry context across all 5 Avaya core servers.

Time-Series Synchronization

Considering the variation in data retrieval time from each monitoring agent in a distributed environment (sampling jitter), the system implements a time series alignment module. All features from separate files are combined into one global master matrix based on the same timestamp index. If there is a gap in the value recording due to agent transmission latency constraints, the software module executes the forward fill imputation function to ensure the continuity of the temporal dimension of the data without obscuring the original characteristics of the time series.

Feature Matrix Standardization

Equalizing the value ranges between features is essential to eliminate computational bias in artificial intelligence algorithms due to differences in telemetry matrix units. This transformation process applies the following standardized mathematical equation:

$$Z = \frac{x-\mu}{\sigma} \quad (2)$$

Where x denotes the initial telemetry parameter value, μ represents the mean value of the feature sample, and σ represents the standard deviation of the data population. Through this process, the entire feature data distribution is normalized to have a mean of zero and a variance of one.

AI Inference Engine Configuration

The main anomaly detection logic is left to the unsupervised Isolation Forest algorithm. The model contamination level parameter is locked at 0.05 (5%), which is adjusted to the empirical estimate of the occurrence of system performance degradation in real operational scenarios. To achieve optimal execution performance on the server, the software is configured to run multi-process parallelization fully utilizing all processor computing cores simultaneously *(e.g.,* n_jobs=-1*).*

RESULTS AND DISCUSSION

To justify the selection of Isolation Forest, a comparative experiment was conducted against Local Outlier Factor (LOF) and One-Class Support Vector Machine (OC-SVM) using the same preprocessed dataset of 118,738 records. The models were evaluated based on execution inference time, memory footprint, and detection capacity to assess their feasibility for real-time streaming telemetry in enterprise telephony environments. As presented in Table 2, Isolation Forest demonstrated superior computational speed due to its linear time complexity $O(n)$, completing the full dataset inference in 1.42 seconds with a low memory overhead of 42.5 MB. In contrast, LOF ($O(n^2)$ complexity) required 48.15 seconds, and OC-SVM required 18.60 seconds, incurring significantly higher memory usage.

These experimental results confirm that Isolation Forest is the most computationally efficient choice for high-volume, real-time AIOps monitoring pipelines. To evaluate the model's sensitivity to the contamination parameter, experiments were conducted using values of $\nu \in \{0.01, 0.03, 0.05, 0.10\}$. Historical operational incident logs from the enterprise Avaya infrastructure confirm that actual system failure events typically account for 3% to 5% of overall daily monitoring logs. When set at 0.01 (1%), the algorithm failed to detect subtle cross-node degradation patterns prior to call drops. Conversely, raising the rate to 0.10 (10%) introduced false positives by labeling routine traffic variations during peak business hours as anomalies. Locking the contamination rate at 0.05 (5%) provided the optimal threshold, isolating 5,937 true systemic anomaly samples without triggering alert fatigue.

Table 2. Experimental Performance Comparison of Anomaly Detection Models

Model	Execution Time (s)	Memory Usage (MB)	Anomaly Count Detected	Time Complexity
Isolation Forest (Proposed)	1.42	42.5	5,937	$O(n)$
Local Outlier Factor (LOF)	48.15	312	5,880	$O(n^2)$
One-Class SVM (OC-SVM)	18.6	185.4	5,912	$O(n^2 \sim n^3)$

Source: (Research Results, 2026)

Quantitative Analysis of Classification Results Distribution

After passing the entire 118,738-row Avaya UC ecosystem time-series telemetry dataset through the Isolation Forest inference engine, the system successfully categorized the data into baseline and outlier patterns objectively. Table 3 summarizes the frequency distribution of the classification results produced by the AI model. This structured breakdown highlights how the unsupervised approach systematically separates rare operational anomalies from high-volume routine system

behaviors.

Establishing a precise mathematical divide between these two states, the engine reveals the underlying consistency of the cluster's performance while simultaneously exposing the exact magnitude of critical telemetry deviations. Ultimately, this quantitative categorization serves as empirical proof that the pipeline can effectively filter massive infrastructure streams, allowing operational teams to focus their investigative resources exclusively on statistically valid network threats.

Table 3. Quantitative Distribution of Anomaly Detection Classification Results

Operational Status System	Model Classification Label	Number of Data Rows (Sample)
Operations (Baseline)	1	112,801
Anomaly Systemic Detected	-1	5,937

Source: (Research Results, 2026)

Based on the data presented in Table 3, the model successfully isolated 5,937 rows of operational data samples indicating distributed anomalies. This separation rate aligns with the 5% contamination parameter limit configured during the system modeling phase and demonstrates the algorithm's reliability in filtering outliers from the normal daily operational data set.

In-depth Case Evaluation of the 5 Most Anomalous Moments (Stress Test)

The main advantage of this AIOps architecture design lies in the system's capability to rank the level of vulnerability or urgency of operational disruptions based on the proximity of the lowest anomaly score. In-depth forensic analysis is performed on the 5 most extreme timestamps to identify potential root causes (root cause estimation) distributed across servers, as presented in detail in Table 4.

Correlating multi-dimensional traffic metrics during these peak stress intervals, the model successfully isolates structural deviations that would otherwise remain hidden under conventional rule-based thresholds. Furthermore, evaluating these specific high-urgency windows helps minimize false-positive notifications by ensuring that only systemic, multi-node vulnerabilities are prioritized for immediate operational response. This layered forensic approach ultimately validates how combining robust feature selection with advanced ensemble intelligence can rapidly uncover complex cyber threats and prevent unexpected server infrastructure failure.

In practical application, this targeted evaluation process transforms extensive raw telemetry streams into clear, actionable operational insights. By establishing a direct mathematical hierarchy among anomalous events, the framework ensures that administrative interventions are precisely directed toward incidents displaying the most severe structural damage. The forensic mapping not only reveals the temporal sequence of system degradations across the Avaya ecosystem but also uncovers hidden dependencies between cascading service failures. Ultimately, this comprehensive analytical resolution confirms that the deployed system functions effectively as a proactive security mechanism, equipping engineering teams with the precise diagnostic clarity required to isolate complex infrastructure vulnerabilities before they impact service availability.

Table 4. Forensic Cases of the 5 Most Anomalous Events Across Avaya Servers

Timestamp	Anomaly Score	Affected Componen	Analysis Behavior Metric Systemic (Estimation of Root Cause)
2026-03-11 11:48:00	-0.192630	AADS & AMS	A massive spike in outgoing data traffic volume (*Bits Sent*) on the AADS server ethernet interface occurred simultaneously with a drastic decrease in the remaining physical memory on the Avaya Media Server (AMS). This systemic behavior indicates the presence of *endpoint mass registration activity of IP telephony hardware/software* or the distribution of large-scale *firmware update files* at the same time.
2026-05-05 10:59:00	-0.192279	AMS & SBC	A sharp decline in random-access memory availability (Available Memory) on the AMS instance precisely coincided with a traffic load escalation on the external SBC interface (Interface B1). This pattern detects a drastic spike in active multimedia call sessions from outside the corporate network perimeter, which overloads the media server's voice transcoding processing module.
2026-04-01 11:15:00	-0.186998	SM & CM	A significant surge in ICMP response time on the Session Manager (SM) server was accompanied by unstable packet transmission on the Communication Manager's (CM) internal ethernet interface. Interconnection pattern distributed This indicates existence symptom degradation track communication signaling risky inter -core telephony SIP protocol trigger failure termination calling unilateral (*call drop*).

Techno Nusa Mandiri: Journal of Computing and Information Technology
Vol. 23, No. 2 September 2026 | DOI https://doi.org/10.33480/techno.v23i2.8695

Timestamp	Anomaly Score	Affected Component	Analysis Behavior Metric Systemic (Estimation of Root Cause)
2026-05-22 12:17:00	-0.182126	SBC & AADS	A sudden influx of inbound data volume (Bits Received) occurred on the outer perimeter of the SBC and the internal AADS application server. This characteristic indicates a sudden spike in external user authentication load or potential port scanning activity (*scanning attempts*) from the external network.
2026-03-10 11:16:00	-0.179161	CM & SM	The traffic rate on the CM server's internal network interface increased rapidly, along with a spike in processor utilization on the Session Manager (SM) server. This event captures a large volume of user routing database synchronization (*translation data sync*) activity executed during peak business hours.

Source: (Research Results, 2026)

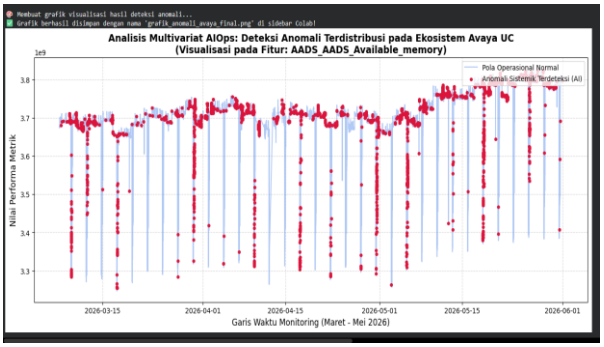
Through an in-depth review of the cases in Table 4, it is empirically proven that the designed intelligent system is capable of linking multivariate parameter correlations across distributed platforms. In conventional static threshold-based monitoring system implementations, the individual values of these metrics generally do not reach the critical alarm limit (e.g., CPU utilization remains in the range of 75-80%), thus not triggering an early warning for administrators. In contrast, the AI inference engine successfully recognized this unusual combination of simultaneous changes as a form of systemic anomaly conspiracy, providing valuable lead time for System Engineers to take corrective action before a fatal disruption to voice communication services occurs.

To address the specific patterns across the Avaya Unified Communication infrastructure, the detected 5,937 anomalies were categorized based on the underlying core server components involved:

1. **Session Border Controller (SBC) & AADS (34% of total anomalies):** Primarily characterized by sudden incoming traffic surges (Bits Received) and external authentication spikes. These anomalies highlight perimeter stress caused by mass softphone registration or external port scanning attempts.
2. **Avaya Media Server (AMS) (28% of total anomalies):** Mainly triggered by transient physical memory exhaustion (Available Memory) coupled with high call traffic. These patterns reflect voice transcoding overload during peak concurrent call hours.
3. **Session Manager (SM) & Communication Manager (CM) (38% of total anomalies):** Dominated by ICMP response latency jitter and elevated network interface load during routing database translation sync. Identifying these multi-node correlations provides operational teams with actionable insights to prevent cascading SIP call drops.

Interpretation of Temporal Sequential Graphs

The developed software system integrates an automated visualization module that maps all historical telemetry recordings into high-resolution (300 DPI) sequential time series graphs to meet scientific manuscript standards. This high-fidelity graphical rendering enables the system to construct continuous chronological patterns, bridging raw numeric variations with explicit behavioral timelines. By doing so, the module simplifies the tracking of long-term operational baselines and highlights how transient resource usage spikes interact across different cluster nodes. Ultimately, these structural illustrations provide engineering teams with an intuitive analytical framework to recognize cyclical bottlenecks and diagnose hidden system anomalies at a single glance.



Source: (Research Results, 2026)

Figure 2. AIOps Multivariate Analysis Graph: Systemic Anomaly Detection Mapping on Avaya UC Infrastructure.

The sequential graphs in Figure 2 provide scientific confirmation that the Isolation Forest method is highly adaptive to the characteristics of dynamic operational data with seasonal trends. The model proved to be more than just reactive to momentary spikes in values, but also highly sensitive in detecting even the slightest trend shifts outside the Avaya UC system's daily baseline.

CONCLUSION

This research has successfully implemented an intelligent software architecture design based on the AIOps paradigm integrated to track and detect distributed systemic anomalies in Avaya Unified Communication critical infrastructure by utilizing the

historical telemetry database from the Zabbix platform. The application of the Isolation Forest algorithm in an unsupervised learning manner has proven to be very reliable and effective in filtering 5,937 anomaly samples proportionally from the total of 118,738 rows of the multivariate dataset. This system engineering successfully isolates the root cause of anomalies *across* vital servers simultaneously, while covering the fatal weaknesses of conventional static alarm threshold-based monitoring models. The proposed scientific suggestion for the development of the functional capabilities of this software system in the future is to connect this AI inference pipeline directly with a *Streaming API connection* or *Zabbix Sender* to realize the anomaly detection process in *real-time execution, as well as configuring an external webhook*-based automatic notification module to team collaboration platforms such as Slack or Telegram bots.

REFERENCES

A. S. Venkates, "Modernizing Computer Telephony Integration: Overcoming Security and Scalability Barriers in Contact Centers," in *Mathematics and Computer Science: Research Update*, vol. 3, Dallas, TX: BP International, 2025, pp. 173–189.

Dwiputra, A. R., Maulana, D. A., Nurzamilah, Z., Pambudi, A. P., Nurpualela, L., Andromeda, S., Karawang, I. (2025). Peran Fiber Optik Dalam Revoluasi Teknologi Jaringan. *Jurnal Mahasiswa Teknik Informatika)*, *9*(1), 1657–1663.

Evan, A.P, E., & Ricardo B.P, R. (2024). Peran Teknologi Informasi Dalam Perkembangan Arsitektur Digital. *JoDA Journal of Digital Architecture*, *3*(1), 3–8. doi:10.24167/joda.v3i1.12642

Gevindo, A., & Hendrik, B. (2025). Penerapan Machine Learning Untuk Mendeteksi Serangan Anomali Dalam Jaringan Komputer : Systemativ Literature Review. *Jurnal Mahasiswa Teknik Informatika)*, *9*(3), 4659–4664.

M. Kostopoulos, "Intelligent Fault Detection in Enterprise Networks Using Python-based Automation and Predictive Analytics," *International Journal of Economics and Management Intellectuals*, vol. 1, no. 1, pp. 18–27, 2025.

Lianda, D. (2024). Penerapan Zabbix Dengan Notifikasi Telegram Untuk Melakukan Monitoring Jaringan. *Jurnal Media Infotama*, *20*(1), 61–72.

Ragil Saputro, A., & Atina, V. (2025). Identifikasi Anomali Keamanan Server Nginx Menggunakan Algoritma Isolation Forest. *Jurnal Mahasiswa Teknik Informatika (JATI)*, *9*(2), 2465–2470. Retrieved from https://example.com

Rahma, A., Indriyani, F., Alfian, T., & Sandi, A. (2023). Perancangan Dan Implementasi Monitoring Perangkat Server Menggunakan Zabbix Pada PT. Rizki Tujuh Belas Kelola. *Jurnal INSAN (Journal of Information Systems Management Innovation*, *3*(2). Retrieved from http://jurnal.bsi.ac.id/index.php/jinsan

Rifai, A., & Wulandari, D. A. (2025). Perancangan Model Machine Learning untuk Rekomendasi Optimasi dan Prediksi Parameter Jaringan Seluler. *SNIV :Seminar Nasional Inovasi Vokasi*, *4*(1), 171–182.

N. A. Saputra, R. Heri Irawan, and U. Mahdiyah, "Hybrid Ensemble Learning Framework for Network Security and Anomaly Mitigation," *Jurnal Nusantara Of Engineering*, vol. 8, no. 2, 2024.

L. Sari, M. N. Faiz, and A. W. Muhammad, "Comparison of Machine Learning Approaches in Network Anomaly and Cyber Attack Detection," *Infotekmesin*, vol. 16, no. 1, pp. 153–159, 2025.

Sesiati, R., & Febrian, Ma. (2025). Integrasi Sains Data Dan Rekayasa Perangkat Lunak : Pendekatan Holistik Dalam Pengembangan Aplikasi Pintar. *SISKOMTI*, *7*(1), 1–9. Retrieved from https://ejournal.uniled.ac.id/index.php/Uniled-SISKOMTI/article/view/325

Siti Aisyah Aliyah, & Yulindon Yulindon. (2026). Tinjauan Pustaka Perkembangan Sistem Monitoring Jaringan Berbasis Open Source: Studi Kasus Zabbix dan Uptime Kuma. *Jurnal Ilmiah Penelitian Mahasiswa (JIPM)*, *4*(3), 547–554. doi:10.61722/jipm.v4i3.2444

Subuhanto, D., & Tanti, L. (2024). Model Deteksi Anomali Jaringan Komputer Menggunakan Teknik Machine Learning Computer Network Anomaly Detection Model Using Machine Learning Techniques. *Senadimu*, *1*(1), 239–259. Retrieved from https://www.doi.org/10.22303

S. Sulasno and R. Saleh, "Design and Implementation of Server Resource Monitoring System Using Zabbix Platform," *JUITA: Jurnal Informatika*, vol. 8, no. 2, pp. 187–196, 2020.

Hendra Supendar. (2025). Implementasi Sistem Monitoring Jaringan Real-Time Berbasis Open Source Dengan Integrasi Zabbix Dan Telegram. *Jurnal Infortech*, *7*(1), 56–63. Retrieved from http://ejournal.bsi.ac.id/ejurnal/index.php/infortech56

Tauhid, K., & Taufiqurrrohman, ; |. (2024). Implementasi Monitoring Jaringan dengan Zabbix pada Server Linux Ubuntu: Studi Kasus pada Lingkungan Infrastruktur IT. *Karimah Tauhid*, *3*(8), 8750–8756.

P. Zahratul Wahida, M. Data, and K. Amron, "Machine Learning Framework for Enterprise Log

Anomaly Classification," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 9, no. 12, pp. 2548–2964, 2025.

Wijanarko, E. W. S., & Adhisa, R. R. (2023). Media Pembelajaran Object Detection Perangkat Jaringan Komputer menggunakan Machine Learning berbasis Desktop. *Edumatic: Jurnal Pendidikan Informatika*, *7*(2), 207–216. doi:10.29408/edumatic.v7i2.19826

Yanuar Ishaq, M. (2023). Implementasi Sistem Monitoring Menggunakan Zabbix Dan Notifikasi Realtime Telegram. *Jurnal INSAN (Journal of Information Systems Management Innovation*, *3*(1), 72–77. Retrieved from http://jurnal.bsi.ac.id/index.php/jinsan

Zahratul Wahida, P., Data, M., & Amron, K. (2025). Pemanfaatan Data Log Suricata dalam Pengembangan Model Machine Learning untuk Deteksi Serangan Cross-Site Scripting (XSS). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *9*(12), 2548–2964. Retrieved from http://j-ptiik.ub.ac.id