AI-Assisted Anomaly Detection for Cybersecurity in IMS Core Networks: A KPI-Driven Study Based on Real-World Telecom Data

Bianca-Ștefania VĂDUVA
Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest, Romania
bianca.vaduva@stud.etti.upb.ro

Abstract

In modern IP Multimedia Subsystem (IMS) core networks, the detection and prevention of cybersecurity threats remain a critical challenge due to the dynamic nature of signaling traffic and the increasing complexity of infrastructure. This paper proposes an AI-assisted anomaly detection approach based on statistical modeling of key performance indicators (KPIs) collected from real-world telecom networks over a one-month period. The analysis targets multiple IMS elements across two major network regions, focusing on Call Setup Success Rate and Total Traffic (Erlang). A contextual z-score model was implemented in MATLAB to monitor these KPIs per hour, enabling the identification of time-based deviations without relying on static thresholds. An alert logic was added to mark days with excessive anomaly rates (>5%) as potentially suspicious. A major traffic spike detected on March 1st is analyzed as a case study, suggesting a possible signaling flood or operational event. The results demonstrate the feasibility of unsupervised anomaly detection in IMS environments, providing early warning signals for cybersecurity-related incidents. This KPI-driven methodology can be extended with advanced AI models for predictive alerting and integration with network management systems.

Index terms: anomaly detection, artificial intelligence, cybersecurity, IMS core networks, KPI monitoring

1. Introduction

The IP Multimedia Subsystem (IMS) has become a fundamental architecture in modern telecommunications, enabling the delivery of multimedia services such as voice, video, and messaging over IP-based networks. As IMS deployments scale to support a growing number of users and services, their exposure to cybersecurity threats has increased significantly [1], [2]. The complexity of signaling protocols like SIP and Diameter makes IMS infrastructures particularly vulnerable to attacks such as signaling floods, malformed messages, and denial-of-service (DoS) attempts [1], [3].

Conventional security mechanisms in telecom environments - such as firewalls, static filters, or signature-based intrusion detection - are often ineffective against dynamic or unknown threats. Even minor deviations in signaling behavior can indicate the early stages of a cyberattack, especially when they impact critical components such as Session Border Controllers (SBCs) or Call Session Control Functions (CSCFs), which are responsible for managing and securing signaling flows [2], [4].

These challenges are further amplified in next-generation telecom environments, where convergence between fixed and mobile networks, together with the integration of IoT and post-quantum resilience concerns, increases the overall complexity and risk surface [5], [6], [7]. In such contexts, traditional perimeter defense becomes insufficient, and monitoring internal KPI behavior becomes a more adaptive way to detect early-stage anomalies.

This work proposes an AI-assisted anomaly detection framework tailored for IMS core networks. The system operates on real-world telecom KPI data collected over a one-month period and focuses on detecting deviations in Call Setup Success Rate and Total Traffic (Erlang). By applying contextual statistical modeling, the framework can identify operational anomalies that may correspond to cyber threats or hidden configuration issues.

The main contributions of this work are: (1) the design and implementation of an unsupervised anomaly detection model adapted to IMS traffic behavior, (2) the use of real operational data from multiple regions to validate the model, and (3) a discussion on how such systems can enhance cybersecurity readiness in telecom infrastructures.

The proposed framework can be extended with more advanced AI models and integrated into existing network management or security information and event management (SIEM) systems for real-time threat detection.

2. Cybersecurity Challenges in IMS

2.1. Signaling Protocol Vulnerabilities

The IMS architecture relies heavily on signaling protocols such as SIP and Diameter, which were not originally designed with strong built-in security mechanisms. As a result, these protocols are vulnerable to malformed messages, spoofing, and denial-of-service (DoS) attacks. SIP floods using REGISTER or INVITE methods can overload Call Session Control Functions (CSCFs), leading to service unavailability and control-plane saturation. This type of vulnerability is especially concerning in legacy PSTN environments that are transitioning to IMS architectures [1], [3]. In addition, attackers may exploit optional or poorly validated SIP headers to bypass filters or cause parsing failures.

2.2. Weaknesses in Implementation and Configuration

Although the IMS standard includes security mechanisms such as IPSec, TLS, and message integrity protection, their implementation is often inconsistent across operational networks. In practice, encryption is frequently limited to access segments, while core or inter-domain links - such as those between SBC and CSCF nodes - may remain unprotected due to performance trade-offs or interoperability constraints [2]. Furthermore, misconfigurations related to DNS resolution, HSS access control, or SIP session timers can expose new vulnerabilities or amplify the impact of otherwise benign anomalies [7].

2.3. Limitations of Traditional Security Mechanisms

Traditional telecom security mechanisms - such as access control lists, static firewalls, and signature-based intrusion detection systems - are generally inadequate for handling evolving and dynamic threat patterns. These tools rely on predefined rules and known signatures, leaving them unable to detect novel or slow-paced attacks. In IMS environments, where even slight deviations in signaling behavior can cascade into large-scale service degradation, this limitation is especially critical [4].

2.4. The Role and Limitations of SBCs

Session Border Controllers (SBCs) play a central role in securing IMS networks, acting as gatekeepers for signaling and media traffic. Their responsibilities include protocol validation, topology hiding, DoS protection, and interconnect policing. However, under high-load or attack conditions, SBCs themselves can become bottlenecks. When operating with static rule sets or limited adaptability, their ability to detect and mitigate emerging threats is significantly reduced [4].

2.5. The Case for Anomaly Detection

To address the limitations of conventional defense mechanisms, modern IMS security architectures increasingly integrate anomaly detection techniques. These approaches monitor real-time traffic behavior, compare it against learned baselines, and flag deviations - rather than relying solely on known attack signatures. When applied to key performance indicators (KPIs) such as Call Setup Success Rate and signaling traffic volume, anomaly detection can help surface otherwise hidden or emerging threats. This capability is particularly valuable in IMS environments, where latency-sensitive services require proactive identification of degradation events [8].

3. Methodology

a. Data Collection

To ensure a practical and representative foundation for anomaly detection in IMS environments, this study utilizes real operational data gathered from a commercial telecom network over a one-month period (February 27 to March 27, 2025). The dataset includes measurements from multiple Session Border Controller (SBC) nodes located in two distinct network regions: Brașov and Cluj. SBCs serve as strategic control points at the edge of the IMS core, where they enforce signaling security, manage routing policies, and regulate access control [5].

The data consists of hourly samples exported from performance monitoring systems, structured across multiple Excel sheets-each corresponding to a specific SBC. Two primary key performance indicators (KPIs) were selected: **Call Setup Success Rate**, representing the ratio of successful call setups to total attempts, and **Total Traffic (Erlang)**, a volumetric measure of signaling load processed by each SBC.

These metrics were chosen to enable both temporal and spatial analysis of network health and to facilitate regional comparisons and node-specific anomaly detection.

b. Feature Selection

The KPIs used in this study were selected based on their operational relevance and direct relationship with signaling behavior and service availability. Call setup failures, for instance, can indicate issues such as signaling errors, registration flooding, or control-plane congestion [2]. Similarly, sudden spikes in traffic may result from replay attacks, malformed signaling bursts, or misconfigured user agents [4].

All features were extracted with an hourly granularity to strike a balance between resolution and noise tolerance. Each KPI stream was treated independently per SBC, with no prior labeling, making the detection process fully unsupervised.

c. Detection Algorithm

The anomaly detection model is based on contextual z-score deviation, calculated independently for each hour of the day. This approach accounts for normal daily variations (e.g., low traffic at night, high peaks in the afternoon) and is robust to seasonality in telecom workloads.

For each data point $x_{i,h}$, where h is the hour, the z-score was computed as:

$$z_{i,h} = \frac{x_{i,h} - \mu_h}{\sigma_h} \quad (1)$$

where μ_h and σ_h are the mean and standard deviation for all data points at hour h. A threshold of $|z| > 2.5$ was used to flag anomalies, which is commonly applied in statistical process control and time series anomaly detection [5].

d. Alert Logic

Beyond individual outlier detection, the system implements an aggregated alerting mechanism at the daily level. For each day, the total number of anomalies is divided by the total number of hourly samples, yielding a daily anomaly rate. Days exceeding a 5% threshold are flagged as suspicious.

This aggregation helps reduce operator overload and aligns with anomaly clustering practices found in modern cybersecurity telemetry systems [8]. Similar logic is used in operational environments where lightweight alerting systems monitor deviations from baseline across multiple nodes and metrics [6].

e. Implementation

The detection framework was implemented in MATLAB, leveraging its high-performance computing and data visualization capabilities. Built-in statistical functions and table structures were used to preprocess KPI streams, compute z-scores, and generate visual outputs.

Each SBC's time-series behavior was visualized individually, with red markers indicating detected anomalies. Additionally, a heatmap was constructed to provide an at-a-glance view of daily alert status across all SBCs. The implementation is modular and extensible, allowing for the inclusion of new KPIs or streaming data pipelines. The unsupervised approach ensures applicability across heterogeneous IMS environments and vendor technologies.

4. Experimental Results

The proposed anomaly detection framework was applied to real operational KPI data from six SBC nodes - three located in the Brașov region (brasbc01, brasbc02, brasbc03) and three in Cluj (clusbc01, clusbc02, clusbc03). The monitored KPIs included Call Setup Success Rate and Total Traffic (Erlang), analyzed independently per node over a one-month period (February 27 - March 27, 2025).

4.1. Detected Anomalies per SBC

Table 1 presents the number of data points analyzed and the anomalies detected per SBC. For the Call Setup Success Rate, most anomalies were detected during off-peak hours - particularly at night and during weekends - when normal variation is more pronounced. In contrast, anomalies in Total Traffic (Erlang) were rare, with only one extreme outlier observed.

Table 1. Detected anomalies per SBC node

SBC Node	Total Points	Anomalies Detected
brasbc01	2689	110
brasbc02	2689	98
brasbc03	2689	94
clusbc01	2689	91
clusbc02	2689	99
clusbc03	2689	118

In addition to the numerical summary in Table 1, the anomaly detection process was visualized for each SBC using a time-series plot with overlayed anomaly markers. Figure 1 illustrates a representative example, where the KPI values are plotted over time, and detected anomalies are highlighted in red.

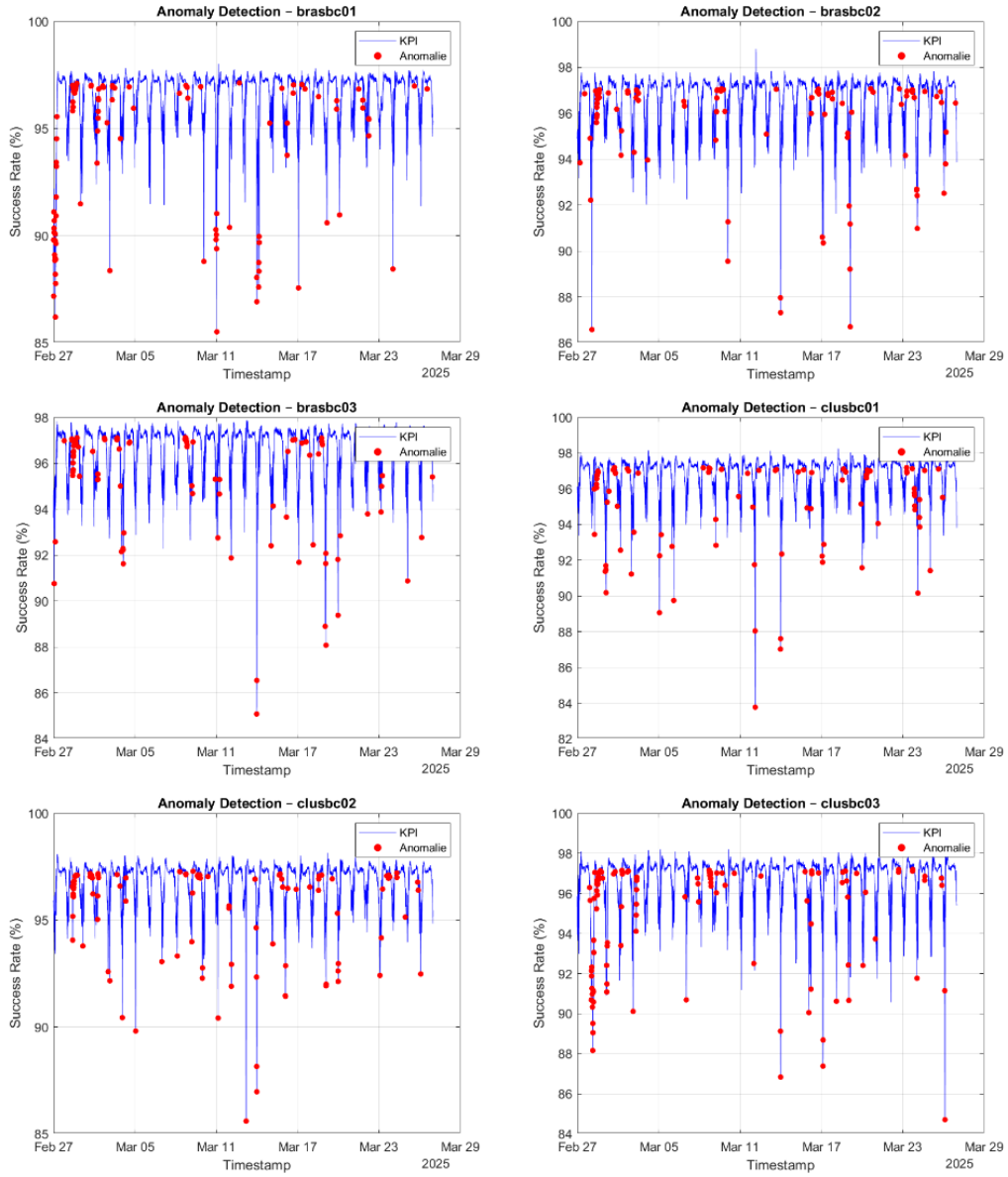

Fig. 1. Time-series anomaly detection for Call Setup Success Rate - sample SBC

4.2. Daily Alert Heatmap

Beyond individual anomaly detection, an aggregated daily alerting mechanism was implemented. For each day, the proportion of anomalous KPI samples was computed, and days exceeding a 5% anomaly threshold were flagged as suspicious. This higher-level abstraction helps reduce noise from isolated outliers and directs attention toward periods of potential operational or security relevance.

Figure 2 presents a heatmap summarizing the alert status for each SBC across the monitored period. Most days were categorized as normal, indicating stable network behavior. However, several isolated alert days were identified, suggesting short-term anomalies, localized performance degradations, or possible low-volume signaling threats.

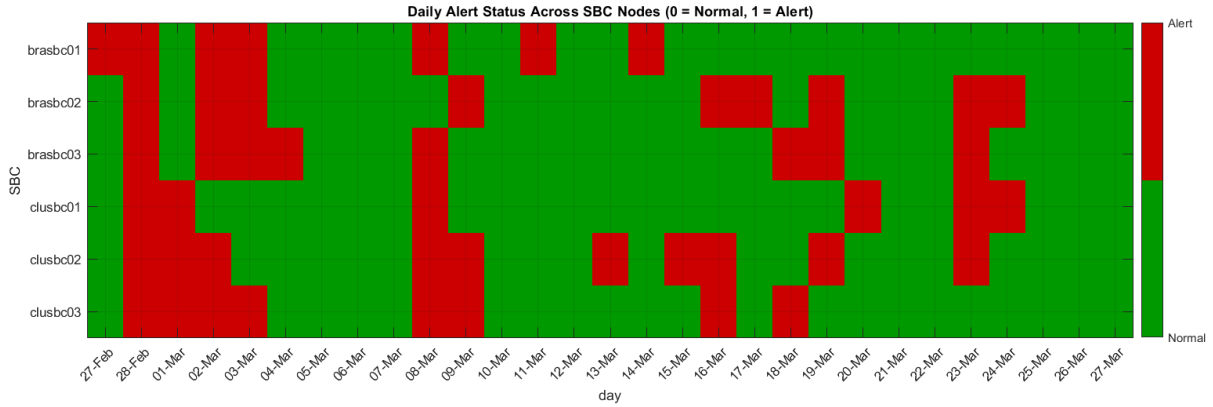

Fig. 2. Daily anomaly alert heatmap (Call Setup Success Rate)

4.3. Spike Detected on March 1st

A significant anomaly was observed on March 1st, characterized by an abrupt spike in Total Traffic (Erlang). The recorded traffic volume on this day was drastically higher than the contextual hourly average, resulting in a z-score exceeding the anomaly threshold by a wide margin. Figure 3 clearly shows this outlier compared to the typical traffic profile for the node.

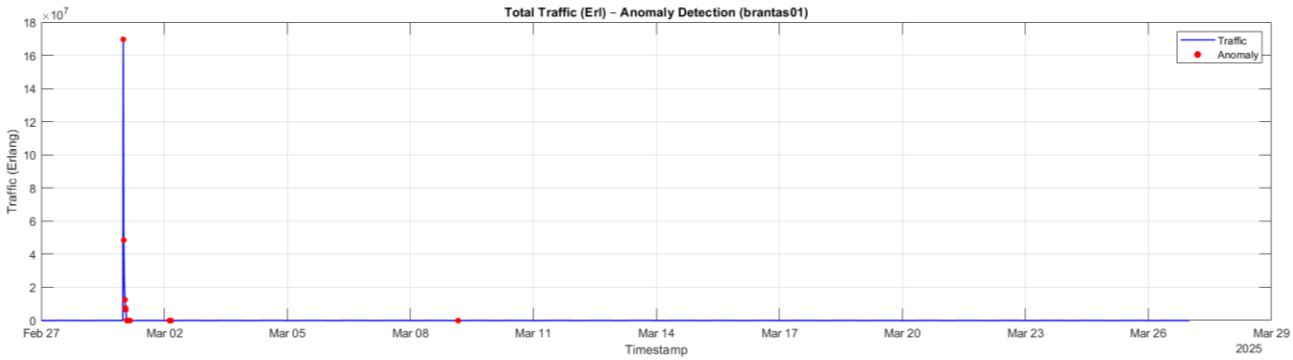

Fig. 3. Anomaly detection - Total Traffic on brantas01

This spike may be explained by an operational event such as rerouted traffic following a failover, or alternatively, a deliberate volumetric attack (e.g., signaling flood). While no correlated degradation in other KPIs was observed, such singular deviations justify investigation and support the utility of anomaly-based early detection strategies [8].

4.4. Comparative Regional Analysis

The comparative analysis between the two regions revealed that Cluj SBCs exhibited a slightly higher anomaly density in the Call Setup Success Rate KPI. This may reflect differences in network configuration, traffic distribution, or signaling load per node. Brașov SBCs displayed greater overall stability, with the exception of the isolated high-traffic anomaly observed on March 1st. These differences underscore the value of localized monitoring, enabling telecom operators to detect and respond to region-specific risks or misconfigurations.

5. Discussion

The experimental results confirm that KPI-driven anomaly detection can serve as an effective early warning system for both cybersecurity incidents and operational issues within IMS core networks. The use of contextual statistical modeling allows for the identification of irregular patterns that might remain undetected by static or rule-based monitoring systems.

a. Interpreting the March 1st Event

The most significant anomaly observed during the analysis period was a pronounced traffic spike on March 1st in the brasbc01 node. This deviation in the Total Traffic (Erlang) KPI is highly unlikely to be the result of normal user behavior. Potential explanations include: traffic rerouting due to failover mechanisms in other network segments, automated bulk provisioning processes or the initiation of a deliberate signaling flood as part of a denial-of-service (DoS) attempt.

Although no concurrent degradation in other KPIs (such as Call Setup Success Rate) was recorded, such isolated traffic surges may indicate early-stage volumetric attacks, designed to probe system resilience without triggering service collapse. Traditional intrusion detection systems (IDS) are often unable to detect such events due to their low signature visibility, but statistical models - such as the one implemented here - can surface them through behavioral deviation [4].

b. Operational Relevance of Detected Anomalies

The anomalies detected in Call Setup Success Rate were predominantly concentrated during off-peak hours, especially at night and on weekends. These may align with routine network maintenance activities or scheduled reconfigurations. However, repeated minor anomalies under light traffic conditions may also reveal: improper session timer configurations, unsolicited external signaling probes or underlying control-plane fragility.

Rather than filtering such events out, the system's ability to detect both acute and low-severity anomalies allows for a layered observability strategy, blending performance monitoring with cybersecurity insight [8].

c. Integration with Existing Telecom Monitoring Systems

A major advantage of the proposed framework is its lightweight, unsupervised architecture, which enables easy integration into existing telecom operations. Since the system does not require labeled training data, it can function alongside traditional monitoring solutions such as NOC dashboards or SIEM platforms.

SBCs and CSCFs already generate extensive telemetry, including detailed KPI logs. These data streams can be used as input for real-time anomaly detection modules. Once deployed, the contextual z-score model can enhance automated alerting workflows and reduce time-to-detection for emerging threats.

d. Limitations and Future Considerations

The current implementation focuses on univariate anomaly detection, analyzing each KPI independently. While effective, this approach does not capture inter-metric correlations. Future work may expand into multivariate anomaly detection, incorporating features like call failure types, signaling latency, and error rates.

Another potential extension involves anomaly classification, distinguishing between types of deviations (e.g., spikes, drops, persistence) to improve alert prioritization.

As more advanced AI techniques become accessible, methods such as isolation forests, autoencoders, or graph-based neural models could be explored to enhance both accuracy and interpretability. Additionally, complementary schemes like cached registration could be leveraged to reduce signaling load and support robustness during anomalies [9].

6. Conclusions

This paper introduced a lightweight, AI-assisted anomaly detection framework tailored for cybersecurity monitoring in IMS core networks. By applying contextual statistical modeling to operational KPI data-specifically Call Setup Success Rate and Total Traffic (Erlang) - the system was

able to identify both high-impact events and subtle irregularities that traditional monitoring solutions often overlook.

The results demonstrate that unsupervised anomaly detection based on z-score deviation is not only feasible but effective for uncovering signaling issues, potential security threats, and operational misconfigurations. The use of real-world data collected from multiple SBC nodes across two geographical regions validated the model's robustness and highlighted key use cases, including an anomalous traffic spike observed on March 1st.

The main advantages of this approach include the ability to detect anomalies without predefined thresholds or labeled data, compatibility with existing KPI monitoring systems and extensibility across different IMS network topologies and vendor implementations.

As 5G networks evolve and post-quantum security concerns grow in complexity, the need for adaptive, data-driven monitoring systems in telecom infrastructure becomes increasingly critical [6], [7].

References

[1]. E. E. Anderlind et al., "IMS security," in Bell Labs Technical Journal, vol. 11, no. 1, pp. 37-58, Spring 2006, doi: 10.1002/bltj.20143.

[2]. H. Pant, A. R. McGee, U. Chandrashekhar and S. H. Richman, "Optimal availability and security for IMS-based VoIP networks," in Bell Labs Technical Journal, vol. 11, no. 3, pp. 211-223, Fall 2006, doi: 10.1002/bltj.20190.

[3]. B. Soewito, O. D. Saiman and F. E. Gunawan, "Internet Protocol Multimedia Subsystem Security Risk Mitigation In Fix Telephone Network," 2019 IEEE International Conference on Engineering, Technology and Education (TALE), Yogyakarta, Indonesia, 2019, pp. 1-6, doi: 10.1109/TALE48000.2019.9225986.

[4]. A. Neureiter, Security Protection of IMS Based Telecom Networks, M.Sc. thesis, Univ. of Applied Sciences Technikum Wien, Vienna, Austria, May 2017.

[5]. A. Sardella, “Building IMS-Capable Core Networks: Backbone Foundations for Fixed-Mobile Convergence,” Juniper Networks, White Paper, Mar. 2006.

[6]. O. S. Althobaiti and M. Dohler, "Cybersecurity Challenges Associated With the Internet of Things in a Post-Quantum World," in IEEE Access, vol. 8, pp. 157356-157381, 2020, doi: 10.1109/ACCESS.2020.3019345.

[7]. H. Kim, “5G Core Network Security Issues and Attack Classification from Network Protocol Perspective,” Journal of Internet Services and Information Security (JISIS), vol. 10, no. 2, pp. 1-15, 2020.

[8]. R. Dean, W. Akpose, W. Zegeye, and F. Moazzami, “Cyber Security Architecture for Networked Telemetry,” in Proc. International Telemetering Conference (ITC), 2024.

[9]. L. Al-Doski and S. Mohan, “A Cached Registration Scheme for IP Multimedia Subsystem (IMS),” Journal of Cyber Security and Mobility, vol. 3, pp. 317-338, 2014.