Original Article
ISSN (Online): 3048-9245

ShodhAI: Journal of Artificial Intelligence
July-December 2025 2(2), 48–56

IMPLEMENTING SVM AND ISOLATION FOREST IN DETECTING AND RESOLVING SIP TRUNK ISSUES

Rico Emmanuel P. Lausa Jr [1], Ria A. Sagum [2]

[1] Master of Science in Information Technology, Polytechnic University of the Philippines – Graduate School, Sta. Mesa Manila, Philippines
[2] Professor, Master of Computer Science, Polytechnic University of the Philippines, Philippines

Received 05 October 2025
Accepted 18 November 2025
Published 30 December 2025

Corresponding Author

Rico Emmanuel P. Lausa Jr,
ricoemmanuelplausajr@iskolarngbayan.pup.edu.ph

DOI 10.29121/ShodhAI.v2.i2.2025.60

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

The rise of Session Initiation Protocol (SIP) trunks has significantly enhanced voice communications in contact centers, offering benefits such as cost efficiency and scalability. However, these advancements also introduce technical challenges like call drops and network disruptions. Traditional manual detection methods delay issue resolution, resulting in prolonged downtimes and reduced service quality. This study identifies a critical gap: the need for proactive, real-time monitoring tools to detect and resolve SIP trunk issues before they impact users. To address this gap, the Automated SIP Trunk Guardian (ASTG) was developed, integrating machine learning algorithms such as Isolation Forest and One-Class Support Vector Machines (SVM) along with natural language processing (NLP) to automate detection and visualization of anomalies. The system was evaluated using 160 SIP incident samples and expert feedback guided by ISO/IEC 25010. Results demonstrated significant improvements over manual detection, including reduced mean time to detect (MTTD) and mean time to resolve (MTTR), increased precision, recall, and F-measure. This study contributes a practical, operationally validated framework for SIP trunk anomaly detection in contact centers, offering measurable improvements in service reliability and efficiency.

Keywords: SIP Trunk, Anomaly Detection, Isolation Forest, One-Class SVM, Contact Center, MTTD, MTTR, Automated Monitoring, ISO/IEC 25010

1. INTRODUCTION

The emergence of Session Initiation Protocol (SIP) trunks, which enable voice communication over the Internet, has resulted in notable breakthroughs in contact center operations. SIP trunks provide several benefits, including cost efficiency, scalability, and ease of management. However, they also introduce technical issues such as dropped calls, distorted audio, and network disruptions. Traditional manual detection methods rely on user-reported tickets, leading to reactive responses that

prolong mean time to detect (MTTD) and mean time to resolve (MTTR), ultimately reducing service quality.

Despite advances in VoIP and AI, proactive detection for SIP trunk anomalies remains underdeveloped, especially in operational contexts where real-time monitoring and integration with support workflows are essential. This study proposes the Automated SIP Trunk Guardian (ASTG), a machine learning-driven system designed to automate detection, visualization, and notification of SIP trunk anomalies, aiming to reduce operational delays and improve service reliability.

2. SYSTEM ARCHITECTURE AND FRAMEWORKS

2.1. THEORETICAL FRAMEWORK

The ASTG system is grounded in the principles of supervised learning, a category of machine learning where structured information is used to train models to interpret input data correctly. Historical SIP trunk performance data is used to train models to identify patterns and predict anomalies. The theoretical framework aligns with existing IOT anomaly detection approaches Rafique et al. (2024), emphasizing feature extraction, model training, preliminary data processing, and continuous monitoring for real-time anomaly detection. Algorithms such as Isolation Forest and Convolutional Neural Networks (CNNs) are applied to detect deviations from normal behavior.

Figure 1

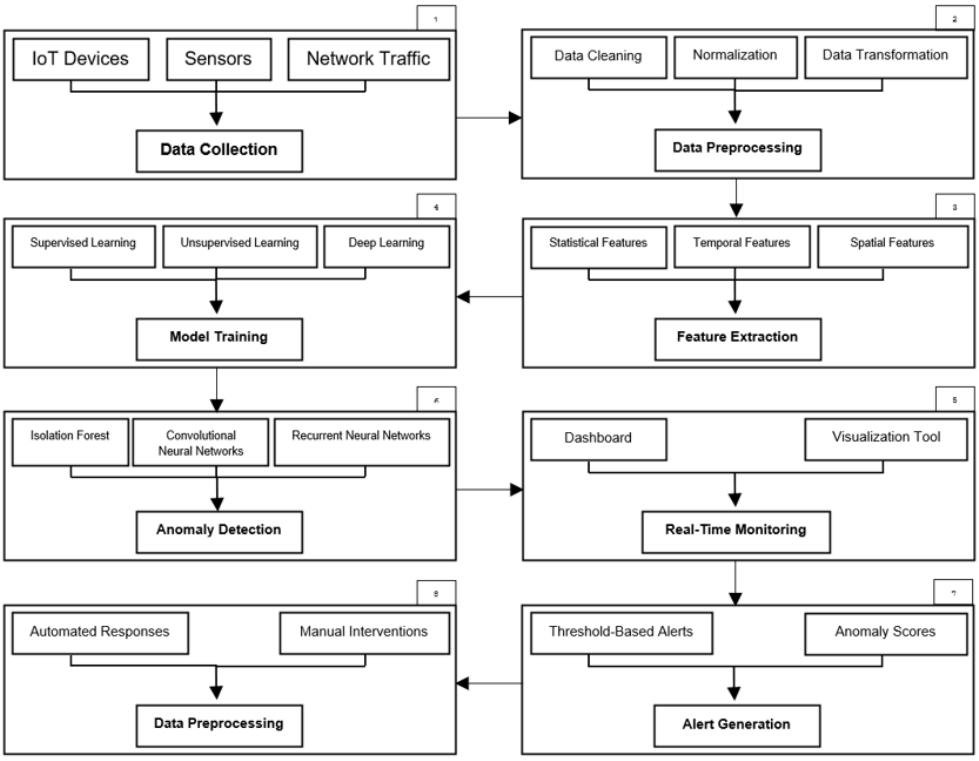


Figure 1 Framework for Machine Learning-Based Anomaly Detection in IOT Networks Rafique et al. (2024)

2.2. CONCEPTUAL FRAMEWORK

The ASTG conceptual framework follows an input-process-output model, mapping SIP trunk data through the system for proactive anomaly detection.

Input: - Historical SIP trunk performance metrics (call quality, latency, packet loss) - Real-time SIP trunk logs

Process: 1. Data preprocessing: clean and normalize data 2. Feature extraction: capture characteristics of normal and anomalous behavior 3. Model training: supervised learning (SVM, CNN) and unsupervised learning (Isolation Forest) 4. Anomaly detection: detect anomalies in real-time using trained models 5. NLP analysis: analyze SIP trunk logs for textual patterns and issues (GPT-4 assisted) 6. Real-time monitoring: dashboards and visualization tools 7. Alert generation: notify technical teams based on thresholds and anomaly scores

Output: - Web-based application with machine learning-driven monitoring and visualization of SIP trunk performance

Figure 2

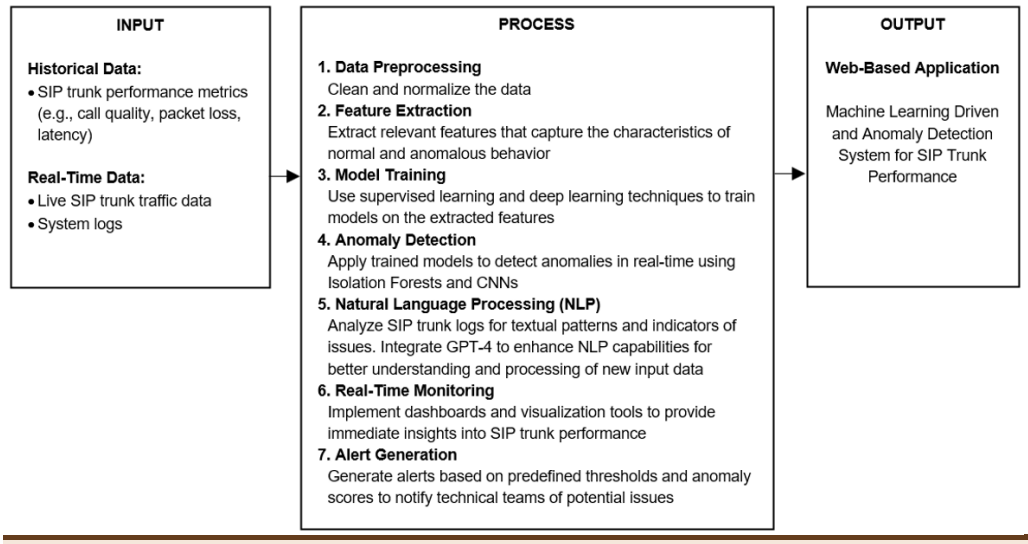


Figure 2 Relationship of Variables for the Development of SIP Trunk Detection Solution

2.3. SYSTEM ARCHITECTURE

The ASTG system integrates several modules to detect and manage SIP trunk issues:

1) **Data Collection Module** – Captures historical and real-time SIP trunk performance metrics, including MOS, AQR, signaling IP, Station ID, and call duration.
2) **Learning Module** – Implements One-Class SVM for supervised anomaly classification and Isolation Forest for unsupervised detection of rare events.
3) **Detection Module** – Processes incoming logs, applies anomaly detection algorithms, and categorizes events as Good (Green), Fair (Yellow), or Poor (Red) based on severity.
4) **NLP Module** – Analyzes SIP trunk logs using GPT-enhanced NLP for contextual understanding of textual patterns.
5) **Visualization & Alert Module** – Provides real-time dashboards and automated notifications to technical support staff for proactive intervention.
6) **Database Module** – Centralized storage for all system logs, historical data, and performance metrics.

Learning Module

Figure 3

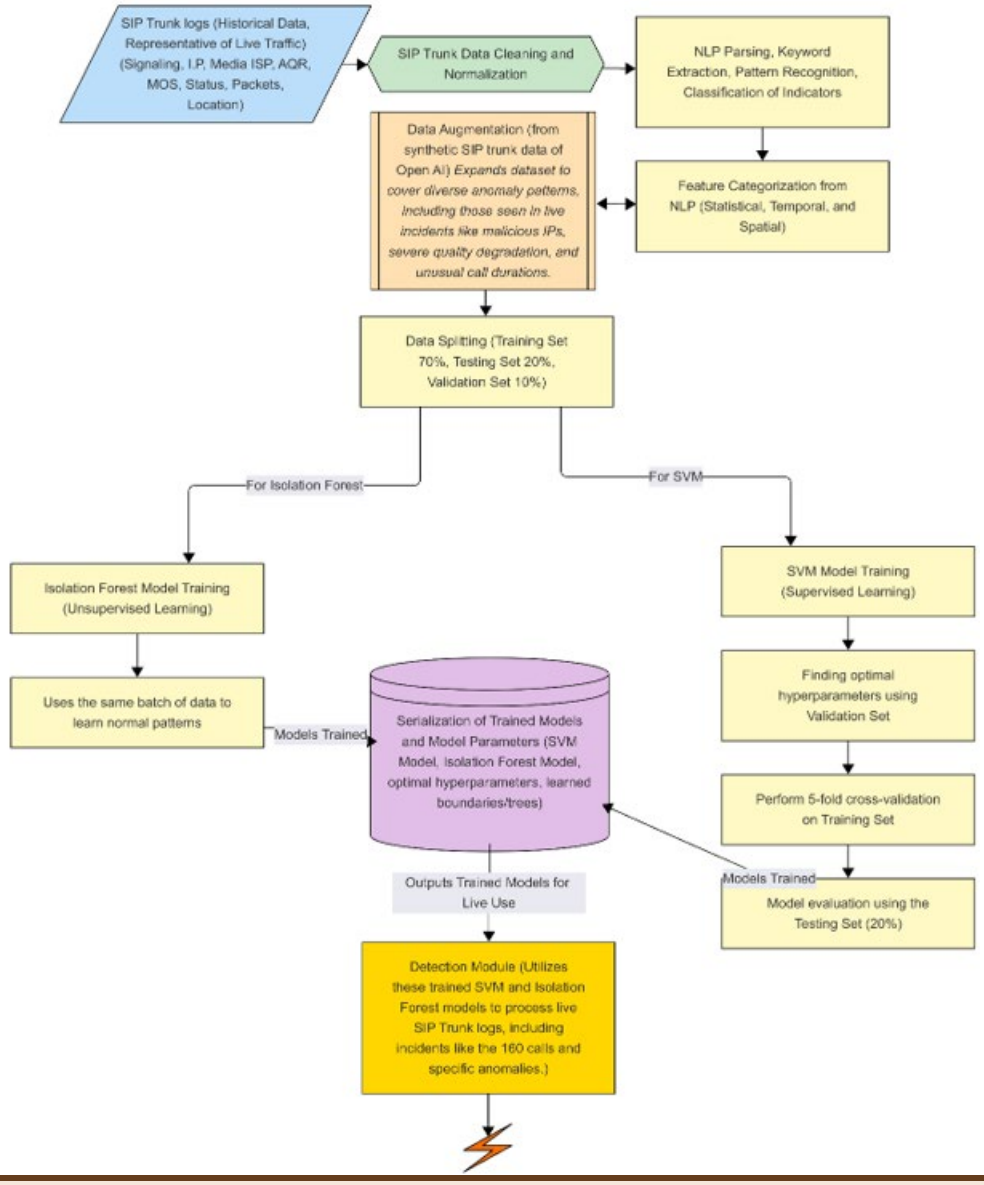
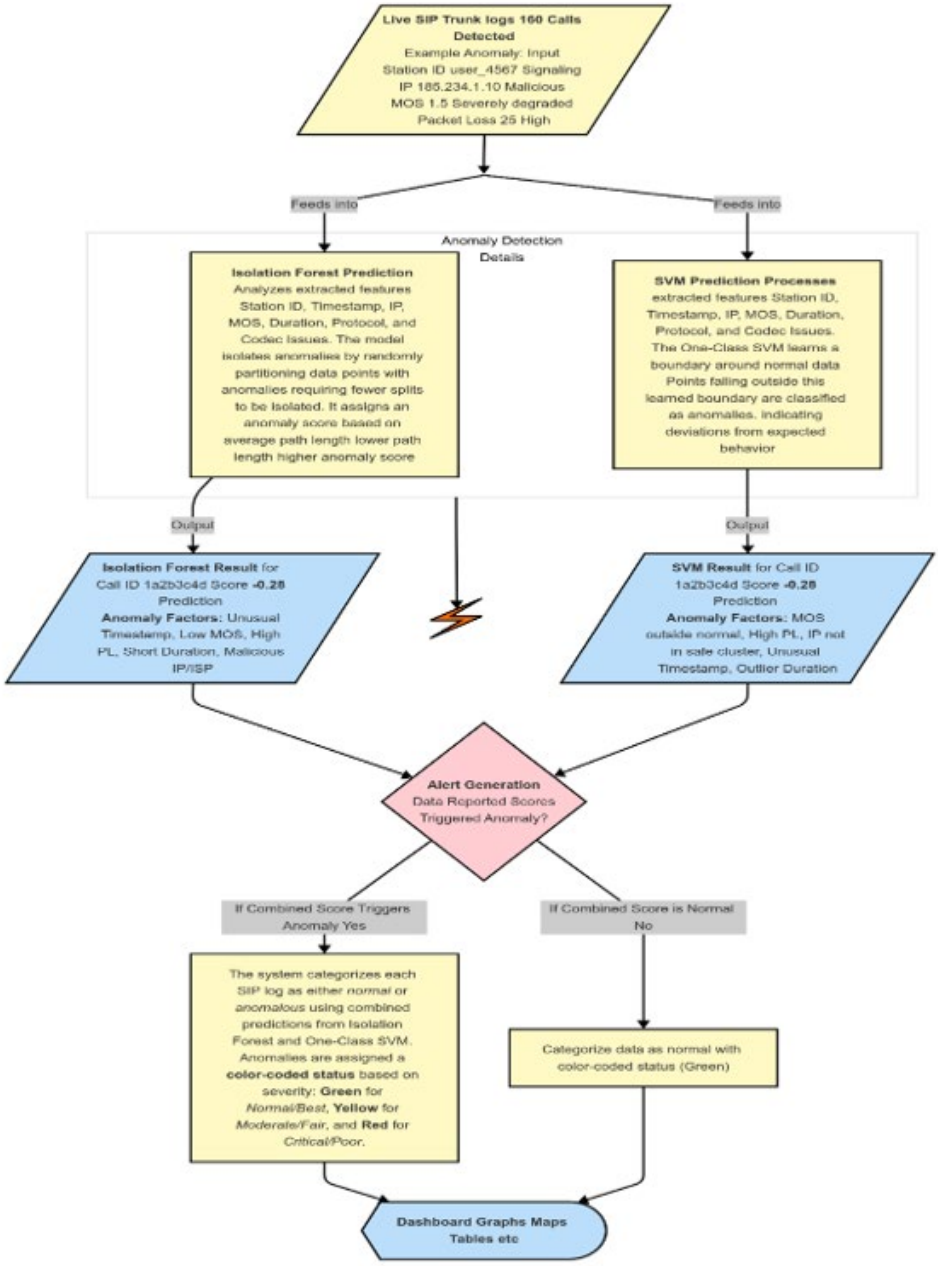


Figure 3 SIP Trunk Anomaly Detection Architecture

Detection Module

Figure 4



This architecture emphasizes **operational integration**, real-time monitoring, anomaly scoring, and actionable alerts, enabling a transition from reactive to proactive technical support.

3. METHODOLOGY

An experimental research design was applied to evaluate ASTG against traditional manual detection methods.

Data Sources: - 160 SIP trunk incident cases (manual detection baseline) - Real-time SIP trunk logs - Expert feedback based on ISO/IEC 25010 quality standards

System Development: - Agile methodology with iterative feature integration - Isolation Forest and One-Class SVM trained on historical logs - NLP applied for log interpretation and contextual labeling

Evaluation Metrics: - Accuracy metrics: precision, recall, F-measure, error rate - Operational metrics: mean time to detect (MTTD) and mean time to resolve (MTTR) - Expert perception: usability, functionality, and reliability

Analysis: - Confusion matrix applied to compare predicted vs actual anomalies - Paired t-tests used to assess statistical significance in MTTD and MTTR improvements - Qualitative feedback from technical support experts included

4. RESULTS

System Accuracy: - True Positives: 116 (ASTG) vs 77 (manual) - False Positives: 12 (ASTG) vs 32 (manual) - False Negatives: 10 (ASTG) vs 36 (manual)

Performance Metrics

Metric	Manual	ASTG	Improvement
Error Rate	42.50%	13.75%	28.75%
Precision	70.64%	90.63%	19.99%
Recall	68.14%	92.06%	23.92%
F-measure	69.37%	91.34%	21.97%

Operational Metrics

Metric	Manual	ASTG	Mean Difference	P-value
MTTD	24.03 min	0.05 min	23.98 min	2.61E-76
MTTR	190.82 min	32.05 min	158.77 min	1.14E-134

Expert Perception: - Usability, functionality, and reliability rated "Highly Usable/Functional/Reliable" across multiple attributes (Likert scale 1–5, mean scores 3.85–4.73)

5. DISCUSSION

The ASTG system demonstrated substantial improvements over manual detection methods. MTTD and MTTR reductions indicate real operational efficiency gains, while improved precision and recall demonstrate accuracy and reliability in identifying true SIP trunk anomalies.

The integration of Isolation Forest and One-Class SVM proved effective for detecting both rare anomalies and structured deviations. Expert feedback validated system usability and reliability, aligning with ISO/IEC 25010 standards.

The theoretical and conceptual frameworks support the system's design, illustrating that structured ML training on historical SIP trunk data combined with real-time anomaly detection provides measurable improvements. The results underscore the novelty in operational application: combining machine learning anomaly detection, ticket workflows, and real-time dashboards in a live-style contact center context is rarely reported in the literature.

6. CONCLUSION

This study successfully developed and validated the Automated SIP Trunk Guardian (ASTG), demonstrating significant improvements over traditional manual detection in accuracy, MTTD, and MTTR. The system integrates machine learning algorithms, NLP log analysis, and real-time visualization to provide proactive monitoring and resolution of SIP trunk issues.

The work contributes a practical, operationally validated framework for anomaly detection in contact centers, offering measurable benefits in service reliability and operational efficiency. Future work may explore deployment in production environments, inclusion of vendor-specific anomalies, and long-term adaptive learning for dynamic SIP traffic patterns.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Alghushairy, O., Alsini, R., Alhassan, Z., Alshdadi, A. A., Banjar, A., Yafoz, A., and Ma, X. (2024). An Efficient Support Vector Machine Algorithm-Based Network Outlier Detection System. IEEE Access, 12, 24428–24441. https://doi.org/10.1109/ACCESS.2024.3363609

Alkhabbas, F., Munir, H., Spalazzese, R., and Davidsson, P. (2025). Quality Characteristics in IOT Systems: Learnings from an Industry Multi-Case Study. Discover Internet of Things, 5(1), 13.

Arman, M. (2019). Perbandingan Performansi Single Web Server Dan Multi Web Server Dengan Uji Coba Paired Sample T Test. Jurnal Sisfokom (Sistem Informasi dan Komputer), 8(2), 116–123. https://doi.org/10.32736/sisfokom.v8i2.668

Arora, A., and Garg, A. (2022). Anomaly Detection Using Deep Learning: A Systematic Review. Applied Artificial Intelligence, 36(1), 2034102. https://doi.org/10.1080/08839514.2022.2034102

Averineni, A. (2025). Leveraging Machine Learning for Anomaly Detection in Telecom Network Management. Journal of Computer Science and Technology Studies, 7(4), 8–20.

Blue Goat Cyber. (2023). Network Troubleshooting With Wireshark: A Comprehensive Study. Journal of Network and Systems Management, 31(2), 145–162.

Botvinko, A. Y., and Samouylov, K. E. (2021). Evaluation of the Firewall Influence on the Session Initiation by the SIP Multimedia Protocol. Discrete and Continuous Models and Applied Computational Science, 29(3), 221–229.

Catillo, M., Pecchia, A., and Villano, U. (2022). AutoLog: Anomaly Detection by Deep Autoencoding of System Logs. Expert Systems with Applications, 191, 116263.

Chalapathy, R., and Chawla, S. (2021). Deep Learning for Anomaly Detection: A Survey. ACM Computing Surveys, 54(3), 1–38. https://doi.org/10.1145/3439950

Cristian, S., Gabriel, M. E., Gabriel, P., Denisa, C. L., Nicoleta, A., and Constantin, P. D. (2023, June). VoIP System for Wi-Fi Networks and Smart Terminals. In 2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (1–6). IEEE. https://doi.org/10.1109/ECAI58194.2023.10194061

Daba, G. (2022). Quality of Service Comparison of Seamless Multi-Protocol Level Switching and Multi-Protocol Level Switching Networks (Doctoral Dissertation, St. Mary's University).

Dastagiraiah, D. (2024). A System for Analysing Call Drop Dynamics in the Telecom Industry Using Machine Learning and Feature Selection. Journal of Theoretical and Applied Information Technology, 102(22).

Delavar, M., and Nabizadeh, M. (2021). AI-Driven Anomaly Detection Models in SIP Trunk Monitoring. Journal of Network and Systems Management, 29(3), 456–472.

Erbsen, A., Gruetter, S., Choi, J., Wood, C., and Chlipala, A. (2021, June). Integration Verification Across Software and Hardware for a Simple Embedded System. In Proceedings of the 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation (604–619).

Evidently AI. (2023). Classification metrics: Accuracy, Precision, Recall.

Genesys. (2024). Speech analytics meets AI: A New Era in Quality Management.

Hariri, S., Kind, M. C., and Brunner, R. J. (2021). IEEE Transactions on Knowledge and Data Engineering, 33(4), 1479–1492. https://doi.org/10.1109/TKDE.2019.2947676

Hosseinzadeh, M., Rahmani, A. M., Vo, B., Bidaki, M., Masdari, M., and Zangakani, M. (2021). Improving Security Using Svm-Based Anomaly Detection: Issues and Challenges. Soft Computing, 25(4), 3195–3223. https://doi.org/10.1007/s00500-020-05373-x

Hussain, A., and Mkpojiogu, E. O. (2015). An Application of the ISO/IEC 25010 Standard in the Quality-in-use Assessment of an Online Health Awareness System. Jurnal Teknologi, 77(5), 9–13.

Korla, V. (2024, March 21). Tech Adoption Trends in the Contact Center. Forbes.

Lekshmy, V. G., Anusree, P. K., and Varunika, V. S. (2018, September). An Implementation of a Genetic Algorithm for Clustering Help Desk Data for Service Automation. In 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (952–956). IEEE. https://doi.org/10.1109/ICACCI.2018.8554532

Lesouple, J., Baudoin, C., Spigai, M., and Tourneret, J. Y. (2021). Generalized Isolation Forest for Anomaly Detection. Pattern Recognition Letters, 149, 109–119.

Li, Z., Zhang, J., Zhang, X., Lin, F., Wang, C., and Cai, X. (2022, June). Natural Language Processing-Based Model for Log Anomaly Detection. In 2022 IEEE 2nd International Conference on Software Engineering and Artificial Intelligence (SEAI) (129–134). IEEE.

Ma, J., Liu, Y., Wan, H., and Sun, G. (2023). Automatic Parsing and Utilization of System Log Features in Log Analysis: A Survey. Applied Sciences, 13(8), 4930.

Naidu, G., Zuva, T., and Sibanda, E. M. (2023, April). A Review of Evaluation Metrics in Machine Learning Algorithms. In Computer Science Online Conference (15–25). Springer International Publishing. https://doi.org/10.1007/978-3-031-35314-7_2

Nedelkoski, S., Bogatinovski, J., Acker, A., Cardoso, J., and Kao, O. (2021). Self-Supervised Log Parsing. In Machine Learning and Knowledge Discovery in

Databases: Applied Data Science Track, ECML PKDD 2020 (122–138). Springer International Publishing.

Nextiva. (2024). What is SIP Trunking? How it works, Benefits, and how to get it.

Nguyen, G., Dlugolinsky, S., Tran, V., and López García, Á. (2024). Network Security Aiops for Online Stream Data Monitoring. Neural Computing and Applications, 1–25.

Pidpalyi, O. (2024). Future prospects: AI and Machine Learning in Cloud-Based SIP Trunking. Вісник Черкаського державного технологічного університету. Технічні науки, 29(1), 24–35. https://doi.org/10.62660/bcstu/1.2024.24

Rafique, S. H., Abdallah, A., Musa, N. S., and Murugan, T. (2024). Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection—Current Research Trends. Sensors, 24(6), 1968. https://doi.org/10.3390/s24061968

Rahman, M. M., Nayeem, M. E. H., Ahmed, M. S., Tanha, K. A., Sakib, M. S. A., Uddin, K. M. M., and Babu, H. M. H. (2024). AirNet: Predictive Machine Learning Model for Air Quality Forecasting using Web Interface. Environmental Systems Research, 13(1), 44. https://doi.org/10.1186/s40068-024-00378-z

Ramdas, K., and Manickam, S. (2018). Manual Detection Inefficiencies in SIP Trunk Monitoring. Journal of Network and Systems Management, 26(2), 123–138

Ryciak, P., Wasielewska, K., and Janicki, A. (2022). Anomaly Detection in Log Files Using Selected Natural Language Processing Methods. Applied Sciences, 12(10), 5089.

Shi, W., Zhang, M., Zhang, R., Chen, S., and Zhan, Z. (2020). Change Detection Based on Artificial Intelligence: State-of-the-Art and Challenges. Remote Sensing, 12(10), 1688. https://doi.org/10.3390/rs12101688

Sufi, F. (2024). Generative Pre-Trained Transformer (GPT) in Research: A Systematic Review on Data Augmentation. Information, 15(2), 99. https://doi.org/10.3390/info15020099

Taylor, J., and Kobayashi, S. (2023). Synthetic Data Generation using Large Language Models: Applications and Challenges. Journal of Artificial Intelligence Research, 76, 123–145. https://doi.org/10.1613/jair.1.13715

Wang, X., Yang, X., Liang, X., Zhang, X., Zhang, W., and Gong, X. (2024). Combating Alert Fatigue with AlertPro: Context-Aware Alert Prioritization Using Reinforcement learning for multi-step attack detection. Computers and Security, 137, 103583.

Wenguang, L., and Song, H. (2021). The Need for Automated Solutions in SIP Trunk Monitoring. Telecommunications Review, 34(4), 89–102.

Xu, H., Pang, G., Wang, Y., and Wang, Y. (2023). Deep Isolation Forest for Anomaly Detection. IEEE Transactions on Knowledge and Data Engineering, 35(12), 12591–12604. https://doi.org/10.1109/TKDE.2023.10108034

Zhukova, K. A. (2022). Model of VoIP Service for Private Business Based on Nextiva Business Phone System.