

# Chapter 11

## Anomaly Detection and Downtime Prediction in Server Logs Using Hybrid Machine Learning


**Swati Gandhi**

*Anantrao Pawar College of Engineering and Research, Pune, India*


**Sharda Yashwant Salunkhe**

*Sharad Institute of Technology, College of Engineering, Kolhapur, India*


**Dipa Dattatray Dharmadhikari**

 <https://orcid.org/0000-0001-7206-5573>  
*Maharashtra Institute of Technology, India*


**Ajit Patil**

 <https://orcid.org/0000-0002-2076-9963>  
*Bharati Vidyapeeth's College of Engineering, Pune, India*


**Yogesh Bodhe**

 <https://orcid.org/0009-0003-5212-2835>  
*Government Polytechnic, Pune, India*


**Sonali Bhoite**

 <https://orcid.org/0009-0002-4737-0669>  
*Vishwakarma Institute of Technology, Pune, India*

**Kuldeep Vayadande**

 <https://orcid.org/0000-0002-0848-5407>  
*Vishwakarma Institute of Technology, Pune, India*

**Rahul Mirajkar**

 <https://orcid.org/0009-0004-8021-7601>  
*Bharati Vidyapeeth's College of Engineering, Kolhapur, India*

### ABSTRACT

*In this paper, we propose a forensic framework that is able to forecast downtime errors at the server level based on anomaly detection to system logs, converted into features according to machine learning (ML) algorithms. We used hybrid of ML model, based on Isolation Forest and One-Class SVM algorithms for encoding nor-*

DOI: 10.4018/979-8-3373-4898-8.ch011

*mal patterns of behaviour systems to annotate deviations from the norm. Detailed log file parsing of any log files of interest, feature extraction, and weighted scoring in combining anomalies were among the actions included in my approach. The hybrid model achieved 99.54% accuracy on real-world live-server log validation data and 95.08% in recall, consistent with individual models, making it a not-so-common occurrence. It identified high-risk periods and scheduled the preventive maintenance. This shows the practical way to bring into predictive IT operations log analysis using ML techniques, which in turn answers a very direct critical need for improved reliability of infrastructure. Future work will be pointed toward this dimension in view of limitations related to dataset scope and sensitivity of models to changes in log format.*

## **1 INTRODUCTION**

Today's IT environment is hybrid clouds and resource deployment cycles that are ever changing, where failure has become possible (Remil et al., 2023). In the context of time, downtime approaches the meaning of time away from its prime for business productivity or profitability as far as an organization is concerned. Very few stakes are higher because, according to industry surveys, the average cost of unplanned application downtime is more than \$5,600 cost per minute (Kothakapu, 2021). Traditional IT monitoring solutions are rule-based/manual and reactive per se. An event is then identified whenever a service degrades or fails. Unlike such methods, big data does not scale in this manner. Therefore, it is time to shift the paradigm towards proactive, data-driven methodologies. System logs provide a rich source of information about the behaviors of IT components (Ram, 2022).

By applying machine learning (ML) to log data, it becomes possible to move from forensic analysis to predictive insights. Artificial Intelligence for IT Operations (AIOps) leverages ML and big data analytics to automate incident management, with the goal of predicting and preventing outages before they affect users (Roy et al., 2015; Bhanage et al., 2021).

By past, network management was based on reactive methods, through which IT teams react to problems when they occur.

One of these approaches has very severe disadvantages. This is predominantly common since, mostly, it results in longer downtimes as the response is initiated at the occurrence of a problem. This approach also fails to suffice the speed and scale in modern network architectures of cloud computing and serverless, with distributed work environments. Therefore, more and more business organizations are relying on a more proactive approach and automated solutions in network management that can predict server downtimes that would obstruct operations before the servers

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/chapter/anomaly-detection-and-downtime-prediction-in-server-logs-using-hybrid-machine-learning/401298](http://www.igi-global.com/chapter/anomaly-detection-and-downtime-prediction-in-server-logs-using-hybrid-machine-learning/401298)

## Related Content

---

### Broad Perspective of Smart Home Technology in 2024

Joseph M. Schulz and Jack S. Scilla (2024). *International Journal of Smart Technologies* (pp. 1-27).

[www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186](http://www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186)

### Broad Perspective of Smart Home Technology in 2024

Joseph M. Schulz and Jack S. Scilla (2024). *International Journal of Smart Technologies* (pp. 1-27).

[www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186](http://www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186)

### Overcoming Hurdles: Navigating Challenges in the Adoption of Smart Logistics

Md Mehedi Hasan Emon (2026). *Emerging Trends in Smart Logistics Technologies* (pp. 197-228).

[www.irma-international.org/chapter/overcoming-hurdles/386047](http://www.irma-international.org/chapter/overcoming-hurdles/386047)

### End-to-End Radiology Report Generation From Chest X-Rays Using Vision–Language Models

G. Vennila, Dinesh Kumar K., S. Anitha and Jariya Begum A. R. (2026). *Medical LLMs and AI in Healthcare: Ethics, Trust, and Clinical Applications* (pp. 193-218).

[www.irma-international.org/chapter/end-to-end-radiology-report-generation-from-chest-x-rays-using-visionlanguage-models/412934](http://www.irma-international.org/chapter/end-to-end-radiology-report-generation-from-chest-x-rays-using-visionlanguage-models/412934)

### Automating Athletic Excellence Through Intelligent Process Automation and Sports Analytics

Mohandass Lingappan, S. Sethu, T. Parasuraman, R. Ramakrishnan, Laishram Shila Devi, Vishnuvardhan Reddy and Ranjith V. P. (2025). *Advancements in Intelligent Process Automation* (pp. 179-200).

[www.irma-international.org/chapter/automating-athletic-excellence-through-intelligent-process-automation-and-sports-analytics/358032](http://www.irma-international.org/chapter/automating-athletic-excellence-through-intelligent-process-automation-and-sports-analytics/358032)