Isolation Forest is widely used in unsupervised log anomaly detection because it requires no labeled data, is efficient, scalable, and effective at isolating rare and subtle anomalies typical in logs.Its dependability and accuracy are well-established through research and industry use, offering high true positive rates and low false positives.

Dependability and Accuracy :

Research studies show high accuracy in anomaly detection using iForest compared to other unsupervised methods.

iForest typically has low false positives, which is crucial in operational monitoring to reduce noise.
Fast execution allows near real-time detection.

Performance depends on proper feature engineering and parameter tuning but is generally robust.

Famous tools using Isolation Forest include Splunk, Elastic Stack, Microsoft Azure Anomaly Detector, Amazon Lookout for Metrics, Datadog, and H2O.ai.

Famous Tools Using Isolation Forest for Anomaly Detection :
Splunk (via Machine Learning Toolkit)

Elastic Stack (ELK) — Elastic anomaly detection uses iForest in ML jobs

Microsoft Azure Anomaly Detector

Amazon Lookout for Metrics

Datadog — anomaly detection modules use iForest

H2O.ai — AutoML platform integrates iForest for anomaly detection

some reachers paper links :

https://www.researchgate.net/publication/342635683_Unsupervised_log_message_anomaly_detection

https://www.sciencedirect.com/science/article/pii/S2405959520300643?

https://www.mdpi.com/2227-9709/11/4/83?

https://arxiv.org/abs/2206.06602?

https://www.analyticsvidhya.com/blog/2021/07/anomaly-detection-using-isolation-forest-a-complete-guide/?