

الجمهورية الشعبية الديمقراطية الجزائرية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي 08 ماي 1945 بسيدي بلعباس
École Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbès



THESIS

to obtain the diploma of **Engineer**.

Field: **Computer Science**

Specialty: **Artificial Intelligence and Data Science (IASD)**

Thesis Title

**Explainable AI for Log Anomaly Detection in
Distributed Systems**

Presented by:
Toumi Adem

Submission Date: **June 2026**
Defended before a jury composed of:

Dr. KHALDI Miloud
Dr. Sidi Mohammed Benslimane
Dr. Mohammed Bekkouche
Dr. ANANI Djihed

Président
Supervisor
Co-Supervisor
Examinateur

Academic Year : 2025/2026

Abstract

Modern distributed systems generate massive volumes of execution logs that serve as the primary observability interface for detecting operational anomalies. As the scale and heterogeneity of these systems grow, manual inspection becomes infeasible, making automated, data-driven approaches essential for system reliability.

This thesis presents the design, implementation, and evaluation of an end-to-end explainable log anomaly detection framework for distributed systems. We engineer eleven model architectures across four paradigms—classical supervised classifiers, deep sequential models, reconstruction-based autoencoders, and Transformer language models—and evaluate them simultaneously on the HDFS, BGL, and Spirit benchmarks under a unified zero-leakage experimental protocol. The framework integrates a preprocessing pipeline with dataset-specific detection units, F1-sensitive threshold optimization, and SHAP and LIME explainability modules. A FastAPI REST backend and an interactive Streamlit diagnostic dashboard demonstrate operational viability.

Keywords— Anomaly detection, execution logs, distributed systems, machine learning, deep learning, explainable AI, operational deployment.

الملخص

تُنتج الأنظمة الموزعة الحديثة كميات هائلة من سجلات التنفيذ التي تُعد الواجهة الأساسية لمراقبة واكتشاف الحالات الشاذة التشغيلية. ومع تزايد حجم وتعقيد هذه الأنظمة، يصبح الفحص اليدوي غير عملي، مما يجعل الأساليب الآلية المعتمدة على البيانات ضرورية لضمان موثوقية النظام.

تقدم هذه الأطروحة تصميم وتنفيذ وتقييم إطار متكامل لاكتشاف الحالات الشاذة في سجلات الأنظمة الموزعة مع التركيز على قابلية التفسير. نقوم بتصميم وتنفيذ إحدى عشرة بنية نموذجية عبر أربعة أنماط: المصنفات الخاضعة للإشراف الكلاسيكية، والنماذج التسلسلية العميقة، والمشفرات التلقائية المعتمدة على إعادة البناء، ونماذج اللغات المحوَّلة. يتم تقييم هذه النماذج في آن واحد على مجموعات بيانات مرجعية (HDFS) و BGL و Spirit باستخدام بروتوكول تجريبي موحد يضمن عدم التسرب. يتضمن الإطار أنابيب معالجة مسبقة مع وحدات كشف مخصصة لكل مجموعة بيانات، وتحسين حساس F1، ووحدات تفسير باستخدام SHAP و LIME. يتم توضيح الجدوى التشغيلية من خلال واجهة خلفية REST FastAPI ولوحة تحكم تشخيصية Streamlit.

الكلمات المفتاحية:--- اكتشاف الحالات الشاذة، سجلات التنفيذ، الأنظمة الموزعة، التعلم الآلي، التعلم العميق، الذكاء الاصطناعي القابل للتفسير، النشر التشغيلي.

Résumé

Les systèmes distribués modernes génèrent des volumes massifs de journaux d'exécution (logs) qui constituent l'interface d'observabilité principale pour la détection des anomalies opérationnelles. Face à l'échelle et à l'hétérogénéité croissantes de ces systèmes, l'inspection manuelle devient impraticable, rendant les approches automatisées basées sur les données essentielles pour la fiabilité des systèmes.

Cette thèse présente la conception, la mise en œuvre et l'évaluation d'un framework complet de détection d'anomalies explicable dans les logs des systèmes distribués. Nous concevons et implémentons onze architectures de modèles réparties sur quatre paradigmes : les classificateurs supervisés classiques, les modèles séquentiels profonds, les auto-encodeurs de reconstruction, et les modèles de langage Transformer. Ces modèles sont évalués simultanément sur les benchmarks HDFS, BGL et Spirit selon un protocole expérimental unifié à fuite nulle. Le framework intègre un pipeline de prétraitement avec des unités de détection spécifiques à chaque dataset, une optimisation de seuil sensible au F1, et des modules d'explicabilité SHAP et LIME. La viabilité opérationnelle est démontrée par une interface backend FastAPI REST et un tableau de bord de diagnostic Streamlit.

Mots clés — Détection d'anomalies, journaux d'exécution, systèmes distribués, apprentissage automatique, apprentissage profond, intelligence artificielle explicable, déploiement opérationnel.