**Anomaly Detection in Microservice Systems Using Autoencoders**

**1. Détails de l’article**

* **Titre de l’article : Anomaly Detection in Microservice Systems Using Autoencoders**
* **Auteurs : Manul de Silva, Sashika Mahadura, Sam Daniel, Lakmal Rupasinghe, Manith Kumarapeli, Chethana Liyanapathirana**
* **Année de publication : 2022**
* **Journal : 4th International Conference on Advancements in Computing (ICAC), IEEE**

**2. Résumé**

Cet article propose un système de détection d'anomalies dans les architectures de microservices en utilisant des autoencodeurs. Avec l'augmentation de l'utilisation des architectures de microservices et des conteneurs, la nécessité d'une observabilité adéquate devient cruciale. Les outils de surveillance traditionnels sont insuffisants pour détecter les comportements anormaux dans des systèmes dynamiques. Les auteurs présentent une approche basée sur eBPF pour collecter des données avancées, et utilisent des techniques d'analyse de données basées sur l'IA pour identifier les anomalies.

**3. Domaine traité**

L’article traite du domaine de **la surveillance distribuée des microservices en DevOps** et du **Machine Learning**. Il s’intéresse à l’optimisation des **outils de monitoring et d’observabilité** pour automatiser la détection des anomalies dans des infrastructures cloud-native.

**4. Problème résolu**

* **Problématique scientifique :**
  + Comment améliorer la détection des anomalies dans les systèmes de microservices en exploitant des techniques avancées d’observabilité et de machine learning ?
* **Problème de société :**
  + Les entreprises utilisent des architectures microservices pour garantir la scalabilité et la résilience de leurs applications, mais elles souffrent d’un manque d’outils efficaces pour détecter rapidement et précisément les incidents.
* **Problème scientifique :**
  + L’article cherche à répondre à la question : eBPF couplé à un modèle LSTM-Autoencodeur permet-il une détection d’anomalies plus efficace que les approches classiques ?

**5. Intérêt d’avoir une solution à ce problème**

* Amélioration de la résilience et de la performance des systèmes microservices.
* Réduction du temps de détection et de résolution des anomalies, essentiel dans un environnement DevOps.
* Proposition d’une alternative plus fine et efficace aux solutions basées sur Prometheus et Grafana.

**6. Approche adoptée**

* **Collecte des données :** Utilisation de eBPF pour extraire des métriques noyau sur l’activité des conteneurs (CPU, mémoire, E/S, appels système).
* **Prétraitement des données :** Normalisation des séries temporelles et extraction de caractéristiques pertinentes.
* **Modèle de machine learning :**
  + LSTM pour modéliser la dynamique temporelle des métriques.
  + Autoencodeur pour détecter les anomalies en analysant l’erreur de reconstruction.
* **Déploiement et expérimentation :** Tests réalisés sur un cluster Kubernetes avec l’application Hipster Shop.

**7. Solution proposée**

L’article propose une architecture hybride composée de :

* eBPF pour une collecte de métriques fine et efficace.
* LSTM pour capturer les tendances anormales des séries temporelles.
* Autoencodeur pour détecter les anomalies en mesurant la reconstruction loss.
* Un seuil dynamique pour classifier automatiquement les événements anormaux.

**8. Discussion**

**8.1 Points positifs**

* Approche avancée et performante combinant observabilité (eBPF) et machine learning.
* Faible impact sur les performances, eBPF étant optimisé pour le noyau Linux.
* Réduction du besoin d’intervention humaine grâce à un modèle auto-supervisé.

**8.2 Manquements relevés**

* Ne prend en compte que les métriques système, excluant les logs applicatifs et les métriques réseau.
* Dépend fortement des hyperparamètres, ce qui peut affecter la précision de la détection.
* Expérimenté uniquement en environnement contrôlé, nécessitant une validation en production.

**9. Intérêt pour mon problème de recherche**

Cet article est directement pertinent pour mon thème de recherche : Approche DevOps et surveillance distribuée des applications basées sur les architectures microservices. Il propose une approche combinant eBPF, LSTM et Autoencodeurs pour une surveillance avancée, ce qui ouvre des perspectives pour une intégration dans un pipeline DevOps et pour une comparaison avec d’autres modèles comme les MLP et Transformers.

**10. Travaux à regarder**

1. Wu, L. et al. (2020). "MicroRCA: Root Cause Localization of Performance Issues in Microservices," NOMS 2020. – Modèle de détection d’anomalies dans les microservices basé sur l’analyse de la performance.
2. Provotar, O. et al. (2019). "Unsupervised Anomaly Detection in Time Series Using LSTM-Based Autoencoders," IEEE ATIT. – Explication approfondie de l’utilisation des Autoencodeurs et LSTM pour l’analyse des séries temporelles.

11. Conclusion

L’article présente une approche innovante pour la surveillance des microservices en DevOps, combinant eBPF, LSTM et Autoencodeurs pour une détection avancée des anomalies. Cette approche pourrait être comparée à d’autres techniques comme les MLP ou Transformers pour évaluer son efficacité en production réelle.