How Can Subgroup Discovery Help AIOps?
Yousef Remil

To cite this version:

HAL Id: hal-03627826
https://hal.science/hal-03627826
Submitted on 1 Apr 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
How Can Subgroup Discovery Help AIOps?

Yousef Remil
INSA Lyon, CNRS, LIRIS UMR5205, France
Infologic R&D, Bourg-lès-Valence, France
yre@infologic.fr

Abstract—The genuine supervision of modern IT systems brings new challenges as it requires higher standards of scalability, reliability and efficiency when analysing and monitoring big data streams. Rule-based inference engines are a key component of maintenance systems in detecting anomalies and automating their resolution. However, they remain confined to simple and general rules and cannot handle the huge amount of data, nor the large number of alerts raised by IT systems, a lesson learned from expert systems era. Artificial Intelligence for Operation Systems (AIOps) proposes to take advantage of advanced analytics and machine learning on big data to improve and automate every step of supervision systems and aid incident management in detecting outages, identifying root causes and applying appropriate healing actions. Nevertheless, the best AIOps techniques rely on opaque models, strongly limiting their adoption. As a part of this PhD thesis, we study how Subgroup Discovery can help AIOps. This promising data mining technique offers possibilities to extract interesting hypothesis from data and understand the underlying process behind predictive models. To ensure relevancy of our propositions, this project involves both data mining researchers and practitioners from Infologic, a French software editor.

Index Terms—AIOps, Data Mining, Subgroup Discovery, XAI

I. RESEARCH PROBLEM STATEMENT

Today’s IT environments are increasingly large and complex, and therefore face significant IT operations and maintenance challenges to keep running efficiently and reliably. While classical engineering mindset focus on how to manually perform tedious tasks and resolve anomalies repetitively, rule-based solutions are not sufficient as they scarcely deal with the tsunami of data IT needs to monitor and cannot deliver predictive analysis and real-time insights and hardly respond to outages early enough [1]. These reasons have sparked the interest toward intelligent and automated platforms capable of learning accurately from large volumes of data to respond proactively to slowdowns and mitigate high-impact outages. However, the software industry is at the early stage of innovating, adopting and trusting these so-called AIOps solutions [2], [3]. A myriad of machine learning models have been proposed for the Incident Management Procedure to help engineers efficiently anticipate and detect outages, identify root causes, and remediate issues. Nevertheless, the best models are generally obscure as they do not convey any explanation of the internal process of making decisions, strongly limiting their adoption and deployment by practitioners. At this point, Explainable AI [4] comes into play and aims at extracting interpretable and relevant patterns from data as well as providing a transparent mechanism that explains how black box models work. In this thesis, we address the mentioned challenges with a promising data mining technique, Subgroup Discovery [5]–[7], which seek to find interesting and interpretable patterns in data w.r.t a target problem. Particularly, we are interested in providing insights and explanations of the process that diagnose and triage incidents in the context of incident management procedure. We proposed two first contributions in that direction [8], [9]. This PhD thesis project is at the cross roads of data mining and software engineering and aim at contributing in both fields.

II. DISCUSSION OF AIOPS STATE OF THE ART

AIOps is a recent and cross-disciplinary research area. Existing contributions are scattered due to the lack of an unified terminology, rendering their discovery and comparison difficult. We carried out an in-depth bibliographic study of AIOps techniques for incident management procedure and we developed an AIOps taxonomy whose different approaches are classified with respect to a target problem. Our procedure is summarized in Fig 1, which consists of four distinct phases, with corresponding time cost to minimize. Incident reporting techniques aim first to detect performance degradation and potential anomalies and then create tickets to record relevant and useful information. Incidents should be prioritized according to their degree of severity [10]–[12]. Sophisticated predictive models have been proposed to detect and rank outages based on KPIs metrics, event logs [13]–[16], and execution traces [17]. Once the incident is reported, a diagnosis of the root cause is performed to locate the source problem that triggered the incident [18]–[20]. It is common for an incident to have been previously reported, hence the interest in grouping similar incidents into buckets [21]. Upon the diagnosis of an incident, the right service team should quickly engage for investigation, which is called incident triage: several approaches were proposed to successfully automate this task [22], [23]. The final step is to bring the problematic service back to a normal state by automatically suggesting appropriate healing and remedial actions based on reported historical issues and also knowledge expertise, known as incident mitigation [24], [25].

III. HOW CAN SUBGROUP DISCOVERY HELP AIOPS?

We briefly illustrate Subgroup Discovery (SD) as follows, considering a dataset where objects are described by attributes, one of which is a class. The goal is to discover interesting patterns or object generalizations such as numerical attribute ranges, that strongly characterize a given class. This basic idea also called *supervised descriptive rule discovery* [7]: it
always correlated with performance degradation (e.g., missing results, we were able to pinpoint query properties that are on our production-environment servers. Through the provided SQL workload that contains more than 140K queries run from the obtained results. The experiments were conducted on the user to interact with the framework and iteratively learn of interest. Furthermore, we integrate a visual tool that enables provide exact and heuristic algorithms to identify subgroups is significantly higher and deviant from the “norm”. We measures whose choice is made by the end-user, e.g. one is the workload. We then integrate a diverse set of interestingness for a numerical representation for each single observation in alerts. Then, we define a suitable pattern language: we opted as performance metrics, environment features, and anomaly we augment queries with other relevant information such to extract important attributes (e.g., tables, fields, predicates), falls to an instance of SD. After efficiently parsing queries some target measures, such as execution time. This perfectly that share some properties only and foster at the same time reveals us several insights on why/how it is difficult to make improvement and new applications are particularly good at identifying these limitations. For example, dealing with multi-objective SD [31] and with labels from a hierarchy [32] is difficult. Second, experimenting with real data of our company with the goal to use our data-centric approaches in production revealed us several insights on why/how it is difficult to make adopt techniques such as Subgroup Discovery, it requires a perfect combination of the three SD axis, along with interactivity, prior knowledge and feedback integration, visualization tools, etc. We already started working on other applications linked to the incident management procedure, namely, crash deduplication [21] and early detection of JVM memory leaks [33]. These are two critical problems for Infologic and here again, we believe that Subgroup Discovery has a high potential w.r.t. the state of the art. 

A. Targeting suspect query fragments in large SQL Workloads

In this work [8], we addressed SQL workload analysis, a crucial task for database administrators to identify schema issues and improve performances. Although DBAs can easily identify queries repeatedly causing performance issues, it remains challenging to automatically identify subsets of queries that share some properties only and foster at the same time some target measures, such as execution time. This perfectly falls to an instance of SD. After efficiently parsing queries to extract important attributes (e.g., tables, fields, predicates), we augment queries with other relevant information such as performance metrics, environment features, and anomaly alerts. Then, we define a suitable pattern language: we opted for a numerical representation for each single observation in the workload. We then integrate a diverse set of interestingness measures whose choice is made by the end-user, e.g. one is interested in a set of queries whose execution time distribution is significantly higher and deviant from the “norm”. We provide exact and heuristic algorithms to identify subgroups of interest. Furthermore, we integrate a visual tool that enables the user to interact with the framework and iteratively learn from the obtained results. The experiments were conducted on an SQL workload that contains more than 140K queries run on our production-environment servers. Through the provided results, we were able to pinpoint query properties that are always correlated with performance degradation (e.g., missing indexes, concurrency issues, etc.).
REFERENCES


