

SCALE: Dynamic Load Scaling via Distributed Trace Analysis

UIUC / CS 598 - Cloud Computing Capstone / Fall 2024 / Milestone 4

John Durkin
jdurkin3@illinois.edu

Kevin Mooney
kmoone3@illinois.edu

Sushil Khadka
sushil2@illinois.edu

Samson Koshy
skosh3@illinois.edu

Abstract

In modern systems, scaling of resources is often carried out by some form of automation. Current state of the art automatic scaling software typically focuses on system generated metrics to gauge which components should be scaled. These metrics typically consist of core resources, mainly CPU and memory utilization. While these are valuable and precise indicators for when resources should be scaled, they often do not provide details of the actual performance of the applications whose resources are being scaled. Distributed traces model entire request or transactions as a hierarchical graph of execution spans, with each span representing a discretely measured point of execution. This trace data can provide direct insight into latencies of processes which may not be caught by system level metric indicators.

To test these claims, we present SCALE, an automated resource scaler that makes scaling decisions based on distributed traces. SCALE first samples trace spans for anomalies in their duration, then delivers those spans to a heuristics based modeling engine. The processor then analyzes those spans against a rule set defined around latency thresholds. If these latencies are breached, SCALE will initiate scaling commands to process orchestration systems. SCALE is evaluated with distributed trace data generated via open-source microservice benchmarks run within a Kubernetes cluster.

1 Introduction

Whether running workloads on remote cloud or on-premises clusters or compute grids, one of the most significant factors that can affect operational expense and capital expenditures is proper resource utilization. On one side of the spectrum, if you are under utilizing resources, wasted cost is obvious in the form of unused hardware and network allocation. On the other side of the spectrum, if you are overutilizing resources this can negatively impact response times causing degradation and failure throughout your application. At the least this can frustrate your client base, while in severe cases cause detrimental production outages, leading to possible irreparable damage to your company or brand.

To combat this, software delivery teams are starting to

lean heavily on dynamic workload scaling. This allows them to utilize resources efficiently and as needed. For full scale cloud workloads, this promotes requesting the optimal amount of resources at any given time, maximizing system throughput when service requests are at their peak and relinquishing those resources during periods of low traffic. For on-premises, while the capital expense of buying hardware cannot be unwound, there is still benefit as you can properly scale varying workloads throughout different periods to better share resources across internal development teams and business units.

While technologies exist to varying degrees to support dynamic load scaling, current implementations seem to have their limits. Many are focused directly on hardware resources such as CPU and memory. If the CPU utilization breaches a certain barrier, then new instances of some computational unit will be spun up. Some take a step deeper and will rely on application generated metrics, although there is a direct overhead in instrumenting the right parts of your application, and making scalers aware of and correlating the correct application metrics to the right scaling actions.

These metrics are often analyzed and applied in different ways. Engines can take a manual heuristics based approach, where operators will often define a set of scaling rules and thresholds based on a working knowledge of the system. Other systems opt to take an automated approach, usually drawing on some form of machine learning to make scaling decisions. The novelty of these systems usually stems in the specific machine learning techniques and models that are utilized. Lastly, while not all, a vast portion of autoscalers are tied directly to a specific orchestration system. Usually this stems from being tied to a specific cloud vendor, such as AWS or GCP. Vendor-agnostic scalers are likely to be tied to a single orchestration system, with Kubernetes being the most common case.

We submit that there is significant novelty in a system which makes use of distributed tracing data to make intelligent decisions based on application performance directly as opposed to simple metrics based autoscaling implementations. We believe that it should be designed in such a way that is not tied to any specific decision-making mechanism or orchestration technology. Instead

the implementation should provide abstraction around these two general areas. The system should instead focus on the need to separate interesting vs. benign trace data. Such a design would allow research to key in on the area of anomaly detection in trace data. This would allow operators to tailor scaling to diverse and heterogeneous architectures. Through our research, we will make a case for SCALE, a system which emphasizes the sampling of distributed tracing for anomalous execution duration. In such cases that anomalies are detected, the processor will generate scaling signals based on the analysis of tail latencies of individual calls within those graphs.

2 Background & Characterization

2.1 Related Works

In our research, we drew particular motivation from gaps in the current state of the art of autoscaling systems pointed out by our fellow researchers. Much of this fell in line with our vision, and helped reinforce the direction we took in our own implementation.

2.1.1 Cost of Implementation

Straesser et al. [1] argue that most state-of-art autoscalers are difficult to implement in production because they are often too complex. Moreover, they often rely on traditional platform metrics, for example CPU based scaling. There are applications where the performance profile is not CPU or memory dominated. In those cases, there is an advantage in scaling based on the combination of both platform and application metrics. Additionally, there is a notable lack of generic, general-purpose autoscalers to address these needs.

As mentioned by Eder et al. [2], there are many different distributed tracing implementations current. One important factor that needs to be considered is the resulting cost of its deployment, especially when it comes to deploying it in a pay-per-use billing model. Also, for practical purposes, it is essential that distributed tracing does not significantly degrade application performance. Eder et al. compares serverless applications executing with and without tracing. It further observed the performance impact - measured in terms of runtime, memory usage, and initialization duration varied across the tools analyzed (Zipkin, Otel, and SkyWalking). It concludes that with appropriate tool selection, the advantages of distributed tracing can be maximized while minimizing performance drawbacks.

2.1.2 MircoScaler

Yu et al. [3] proposed *MIRCOSCALER* that aimed to identify the services that need scaling to meet SLA requirements. it achieves this by collecting service metrics

(QoS, i.e. latency) in service mesh enabled architecture by injecting proxy sidecars alongside each microservice application. Although this method is novel, it makes scaling decisions solely based on latency and uses sidecars to collect the metrics.

This is not to say that all autoscaling decisions are based on simple approaches like monitoring CPU, memory, or latency. There has been study, such as the study done by Thanh-Tung et al. [4], in which the authors use Prometheus Custom Metrics (PCM) to collect HTTP request metrics. The collected metrics are then compared against Kubernetes Resource Metrics (KRM) and its impact on Horizontal Pod Autoscaler (HPA) in Kubernetes is analyzed. The authors note that using metrics obtained from PCM increases the effectiveness of HPA but falls short in mentioning how PCM can be used to identify resources which might be a potential candidate for autoscaling.

2.1.3 TraceMesh

One of the more influential works that inspired us was presented by *TRACEMESH* [5], which details a framework for fast and efficient sampling of streaming distributed traces. The model works by first encoding the traces into vectors. This is done by taking a set of traces in a micro-batch, and enumerating each linear call path within the entire set of traces in that batch, and mapping those paths to an index into a vector. A vector is then populated for each trace, by taking the latency to log base of 10 of the tail span of each of its call paths, and populating the value at the index corresponding to that respective path. If a given trace does not contain the path for a given index then a zero is populated.

The next step in this process sketches the vectors onto new vectors of a fixed length. The reason for this is that each micro-batch may likely produce vectors of varying length on each run. As these vectors eventually are fed to a clustering algorithm, each element is treated as a feature. Given this, we want to feed in a uniform set of features to the algorithm, so that we do not have to extend or truncate already fed vectors and likely retrain the model. This sketching is performed using a locality sensitive hashing algorithm, implemented from the works described by *STREAMHASH* [6]. This sketches the original latency value based vectors into fixed length bit vectors. In additions to the reasoning above, this also provides for very memory-efficient data structures.

The final step in the model is to sample the traces via evolving clustering. For this, *DENSTREAM* [7], a density based clustering algorithm. In the algorithm, multiple micro-clusters are introduced. A core micro cluster is introduced for the entries which do not pose as anomalous. Then several smaller outlier micro-clusters exist to identify anomalies. As the model is evolving, the clusters

are pruned to guarantee the weighting of each, and hence the model adapts to new traces which may no longer pose as anomalies. This is often due in part to yet to be seen call graphs, possibly from new services or the like, being introduced to the model.

The work detailed by the authors was very important in our initial understanding of how we should introduce learning models to identify trace anomalies. In fact early implementations of our implementation of SCALE made direct use of *TRACEMESH* until such point that we devised our own methodology for sampling traces.

2.2 Distributed Tracing vs. System Level Metrics

It is our intention to describe an application architecture where one could apply several strategies for autoscaling based on performance based observability data. This could be via a heuristics based or automated (i.e. machine learning) approach. The observability data could come from a number of sources including log data, distributed traces, application metrics or process orchestrator metrics. We will then provide the reader with some example scenarios that could induce actions from an autoscaler. Our examples do not seek to argue the merits of one processing approach over the other.

The examples instead portend to show a benefit in utilizing distributed tracing data for driving auto- scaling decisions. We approach this from the lens that current state of the art autoscalers rely for the most part upon process orchestrator metrics to drive their scaling. The aforementioned metrics are often confined to physical resources such as CPU or memory utilization, and in some cases IO throughput degradation. We present the reader with a sample architecture in Figure 1 that shall allow us to describe instances where distributed traces would likely provide more robust scaling decisions versus system metrics based counterparts.

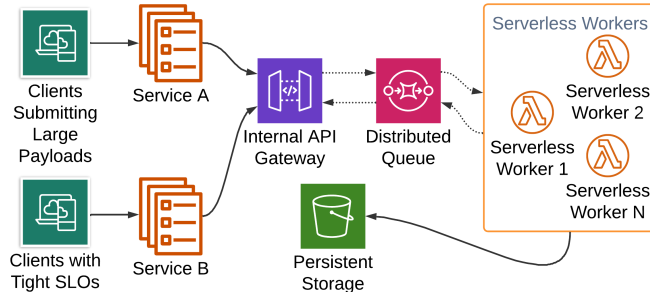


Figure 1: Sample Scalable Architecture

Let's start with two separate microservices, Service A and Service B. While the various details of their upstream clients are of little concern to the example, we do focus on one important characteristic for each. The first is that

clients to Service A typically send very large payloads in their requests (let us say 5MB on average). The second is that clients to Service B have extremely tight SLOs (let us say 500ms). Both services may do some arbitrary processing on the payloads, which for the example let us assume takes negligible time, and then sends some portion of that processing to the same endpoint of an API gateway. The API gateway then forwards these to a distributed queue to be further processed by a set of serverless workers. The main task of the serverless workers is to provide some validation of each payload and finally persist it into an arbitrary data store. We shall examine two scenarios, both which stem from slow processing by the serverless functions. autoscalers using typical orchestration or system level metrics could easily, under certain scenarios, be lead to take misguided scaling actions.

In the first scenario, let us imagine that persistence under optimal circumstances takes on average 100ms. In this scenario, let us imagine that we have capped ourselves to 100 serverless instances. At some point during the system's operation, the system experiences a spike in traffic and begins to see more than 1000 requests per second total between the two microservices to the API gateway. As we only have 100 instances, and it takes 100ms on average per request for a serverless function to handle a request, we will begin to see a backup in the queue. As this back pressures all the way back to the microservices we can picture multiple occurrences. Service A will begin to ramp up in memory usage as it has to buffer large payloads. Service B will begin to miss SLOs, likely resulting in timeouts if they are configured. This could result in a spike in CPU as clients continually attempt retries and these retries begin to stack with legitimately new requests.

The question then is, how would a system level metrics scaler react. It may see that memory is ramping on Service A and begin to vertically scale to more memory for the service. It may see that CPU has spiked on Service B and vertically scale the service. Furthermore, it may see that connections to Service B are stacking due to the timeouts and horizontally scale B. Depending on buffering and back pressure semantics in the API gateway, this scaling could also cascade to the gateway as well. If we could examine a complete distributed trace from Service A or Service B all the way through to persistence, it would be clear the bottleneck is with the serverless functions. From there one can further observe that the functions themselves do not have high latency in processing nor in persistence. A scaling system can then make the correct judgment that it is just the cap on our serverless instances and scale those horizontally.

One can make a simple counterargument to the above, in that we could simply monitor a metric that represents how many requests are sitting in the distributed queue.

If the queue is backed up by some fixed amount, we too can scale. The issue with this approach is that it only provides insight into the latency of the serverless function itself. Is the real issue that some piece of code is running slow due to intense computation or is the function waiting in some blocking IO operation? To further this argument, let us envision a scenario in which database transactions are stacking up, and the database cannot process them all in a timely manner. By utilizing a queue size metric, we simply would have scaled the serverless functions out. This in turn would only serve to further degrade the database. If we were to view a full trace, and we had a trace span directly around the call to the database, we would know the problem is the database itself and can properly scale database resources.

The above examples are not meant to completely discredit analysis of system and infrastructure based metrics as a driver for autoscaling decisions and solutions. Their purpose is show the practicality of leveraging distributed tracing to paint a broader canvas of the health and operation of a distributed system. Well-placed metrics alone could theoretically be pieced together to achieve the same insights as the aforementioned examples. However, this would require very intimate knowledge of your entire dependency graph and for these relationships to be maintained in your monitoring rule set. For smaller systems this may be feasible, but for real-world distributed systems which are composed of hundreds of different services and supporting infrastructure this is untenable. Distributed tracing carries service dependency graphs inherently and so system designers and monitoring software do not have to be fully aware of this graph, and it can easily adapt over time.

2.3 Human Insight vs. Machine Learning

When surveying the landscape of current autoscaling systems available, one of the more significant choices that arises is whether to take a heuristics based approach or whether to use a fully automated approach. Many original scaling systems were based off of Heuristics. It is of course easier to implement a simple rules based parser than to design a fully automated system. This allows you to make use of common domain knowledge and directly apply scaling semantics that you think best serves the health of your system. This of course has some obvious drawbacks. The most important of these is the constant human intervention. You will no doubt have to spend well focused man-hours devising your scaling rule set and then whatever time it takes to put pen to paper. This is also not a one-off cost. As your system changes over time either due to planned architecting or unforeseen circumstances, you will constantly need to rework your scaling model. Looking past the manual overhead this approach brings, there is also the fact that humans are not infallible, and any scheme they come up with, while

hopefully sound, is quite unlikely to be fully optimal.

Several of the more current papers we researched opt to take some form of automated approach. As AI and ML are the hottest subjects in computer science, both academically and commercially, this direction is inevitably explored at great length. Typically, the major differences in these papers is around what machine learning techniques to use. Some systems, such as FIRM [8] and AWARE [9], take a reactive approach, often leveraging reinforcement learning. In this approach, a sort of feedback loop of learning is used, where each scaling action results in a new environmental state and rewards are assigned to each transition to determine if a more optimal state was obtained. As time progresses, the system can take actions based on prior rewards that are more likely to transition to the most optimal state.

Other systems take a more proactive approach. For instance, Madu [10] uses regression techniques backed by TensorFlow to generate predictive models that can sense load before or as it is ramping up to attempt to prevent degradation before it happens. While both of these approaches address the prior issue of added human overhead through automation, they still cannot truly guarantee optimal scaled state at all times. What's more is that ML based solutions often introduce a great deal more complexity due the extra components they often require, as well as the overhead of initial model training as well as retraining to cope with systematic change.

This then brings us to the choice, should we use the insightful approach or the machine learning approach when both analyzing observability data and making scaling decisions within SCALE. Indeed, many highly effective state of the art autoscalers take a heuristics based approach, and as stated most new research seeks to justify moving to an ML based framework. Yet, there is no concrete evidence that one is an order of magnitude better than the other. In fact, one of the most compelling works we read [11], takes this head on. In their paper, they present a strong argument that the most effective system makes use of both, and ML only approaches typically only provide a shifted version of the original training data. Even certain ML based solutions make at least in part some use of human insight, such as AWARE [9] which utilizes a heuristics approach in its offline training mode. Taking all of this into account, this inspired us to use a hybrid approach with SCALE, in which we use machine learning to sample for anomalies and a heuristics based approach for performing strict analysis and decision making.

3 SCALE Design

3.1 Overview

In agreement with the statements and observations outlined in §1 and §2, we introduce SCALE, a software

system which analyzes various system and application generated observability data in order to perform dynamic scaling of application work loads in cloud hosted and/or on-premises environments. We envision a monitor that can make use of open technologies to probe distributed tracing and metric data. This system would wire up to client APIs of a diverse set of process orchestration software. This can include container orchestrators, serverless function controllers or VM provisioning frameworks amongst others. Based on processing of the observability data, a processor will make vertical or horizontal scaling decisions. These decisions will then be communicated to the orchestration systems via their client API to carry out the scaling action.

We are proposing a more adaptable solution than the current state of the art. One that works well with multiple open source technologies as well as proprietary cloud APIs, thus making it more portable across different cloud providers or on-premises orchestration platforms. Most development teams today instrument their applications in some form for distributed tracing, metrics collection or both. In addition, orchestration platforms, web and network proxies and virtualization systems expose a myriad of system level metrics. These all amount to data points which can be used for real time monitoring, trend research and performance analysis. However, these same data points could in turn be analyzed, and when combined with a rich set of thresholds and rules provided by development or operational teams, or by automation and machine learning, be the driver behind dynamic resource scaling.

While we aim for extensibility, the true novelty of our research hinges on the viability of making scaling decisions based on distributed tracing data. Hence, our implementation will directly focus on the consumption, sampling and analysis of traces. The analysis centers around a heuristics based trace processor which will check trace spans for latency breaches above configured thresholds. Based on actions attached to those thresholds, when breached, the processor will initiate scaling directives via a shim that sits atop of the Kubernetes API.

3.2 Architecture

Figure 2 represents the core architecture of SCALE. The three major components which make up SCALE itself are the *sampler*, *processor*, *orchestration shim*. These components work together to form a cohesive, modular workload scaler.

The components are built as implementations upon abstractions allowing for future adoption of other sampling algorithms, decision-making models or orchestration technologies. SCALE is also dependent upon a distributed trace storage mechanism and a distributed trace delivery mechanism. For these we use Grafana Tempo and OTEL

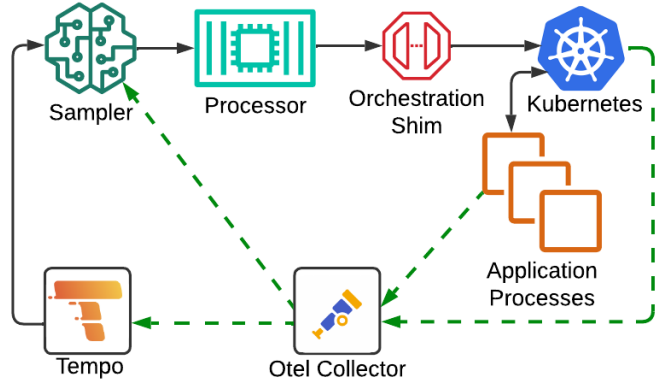


Figure 2: SCALE Architecture

Collector respectively. Much of the communication between components happens over a protocol standard for distributed traces known as OTLP.

3.2.1 OpenTelemetry & OTLP

The fundamental component of the SCALE workflow is a distributed trace. The most common state of the art way to model distributed traces is via OpenTelemetry¹. *OpenTelemetry is a collection of APIs, SDKs, and tools. It is used to instrument, generate, collect, and export telemetry data (metrics, logs, and traces) to help you analyze your software's performance and behavior [12]*. OpenTelemetry provides a uniform data schema for modeling distributed traces as well as serialization in JSON or protocol buffers. Traces are modeled conceptually as a hierarchy within a DAG. Each measured operation of a distributed trace is referred to as a span. A trace is provided with a unique trace id. All spans share the trace id, and in addition contain their own span id. Each span also holds the span id of its parent (unless it is the root span), the start and end timestamp of the span, as well as other various metadata.

In addition to the schema model, a protocol for sending and receiving traces is provided. This protocol is known colloquially as OTLP and is offered over either HTTP REST or gRPC transport. SCALE as well as its supporting components make direct use of both the protocol buffer schema as well as the OTLP gRPC transport. This allows us to model and pass telemetry data throughout the system in a uniform manner, as well as not tying SCALE directly to any specific supporting component.

3.2.2 Collector & Tempo

In addition to OTLP and its accompanying schema, OpenTelemetry provides Collector², a *vendor-agnostic way to receive, process and export telemetry data [12]*. In

¹<https://opentelemetry.io/>

²<https://opentelemetry.io/docs/collector/>

SCALE's case it allows us to build a pipeline for distributed traces. The source of these traces can be either applications or infrastructure. In the case of SCALE it would be microservices or batch jobs running in Kubernetes. In addition, Kubernetes components directly support emitting traces giving you insight into performance of the kubernetes API and kubelets. Collector can be extended to receive traces from sources other than those supporting OTLP, and in fact it currently has support for dozens of other ingestion mechanisms. Thus, while SCALE itself is implemented over OTLP, upstream distributed traces can be generated via a number of different methods.

As traces are sent into Collector, they are then in turn sent downstream to multiple components in the SCALE environment. One of those components is Grafana Tempo³, *an open source, easy-to-use, and high-scale distributed tracing backend* [13]. Tempo facilitates storing and querying of distributed tracing data. In the case of SCALE, the storage backend configured for Tempo is local disk, however in large scale production environments this can be made to point to various object stores such as S3 or GCS. The flow of data from applications and Kubernetes, to Collector, and ultimately to Tempo can be seen in figure 2, represented by the green dashed lines. There is one additional line in this workflow, to the sampler, which we describe next.

3.2.3 Sampler

The sampler is the first direct SCALE component within the architecture's overall pipeline. The job of the sampler is to sample trace spans for anomalies before they are sent downstream for scaling determination. This allows SCALE to predetermine interesting traces in a fast manner, so that extra resources are not wasted on a deep analysis of the call graph. Downstream the SCALE processor relies on a heuristics based examination of traces. However, there is a non-insignificant overhead involved in analyzing large call graphs that should be avoided if possible. This would be further exacerbated if the processor (described in §3.2.4) were swapped for an implementation that relied on a more compute intensive approach.

At its core the main purpose of the sampler is to identify trace spans that have unusual durations. Many of the researched works attempt to perform a holistic sampling of distributed traces. This is often to identify anomalies in both newly seen call graphs in addition to call durations. In our case we are only interested in anomalies in the duration of calls. Given this our sampling is performed directly on each span individually. This leads to both a more deterministic and more performant implementation.

Each span in open telemetry contains four distinct attributes that are important to our sampling. The first of

these two are the service name and operation name. The service name is taken to mean a collection of instances of a specific service as opposed to a single running instance. The operation name denotes a specific unit of execution within a service. Together these help us to uniquely identify very specific call points within a distributed system for classification. The second of the two attributes are start and end time in nanoseconds since Unix epoch. These allow us to determine the duration of the span.

The sampler uses Half-Space-Trees (HS-Tree) [14] to perform anomaly detection on the durations of spans. An online variant of isolation forests, HS-Tree provides a model for fast one-class anomaly detection within evolving data streams. With HS-Tree you provide bounds on the data space which features can fall within. Multiple trees are then formed based on whether features fall within one half of the bound or the other, with different trees holding different orderings of features. All trees are sampled, and a prediction is formed from a consensus of the results from all trees. HS-Tree is best suited for cases where anomalies are rare which is the expectation in distributed trace data. A number of proven open source implementations exist, and for SCALE we chose to go with from River⁴ an online machine learning library for Python.

To categorize the service and operation name we use one-hot encoding. The river HS-Tree implementation is able to accept a sparse python dictionary that does not contain the entire feature set of your data space. Given that we simply use simple numerically increasing integers as keys for the feature name of the service and operation. The general implementation is as follows:

```
encodings = {}

def one_hot_encode(service, operation):
    call_name = f"{service}:{operation}"
    encoding = encodings.get(call_name)
    if encoding is None:
        encoding = len(encodings)
        encodings[call_name] = encoding
    record = {str(encoding): 1}
    return record
```

We then take the difference of the end timestamp minus start timestamp and scale these to milliseconds. This is added as a second feature to the record and passed into the River HS-Tree model for sampling. To initially train the HS-Tree model, a pre-configured set of traces are queried from Tempo via an HTTP REST service which provides traces in OpenTelemetry protocol buffer format.

³<https://grafana.com/oss/tempo/>

⁴<https://riverml.xyz/dev/>

The traces are stored in a pandas data frame as they are collected. When all traces have been pulled, the model is trained which each span featurized as per the above described algorithm. The sampler has six core parameters which are used to calibrate the model prior to training:

Table 1: Sampler Parameters

Parameter	Description
n_tree	number of HS-Trees
height	height of each HS-Tree
window_size	observations in each HS-Tree node
min_score	minimum score required for sampling
max_duration	maximum bound for duration feature
train_size	number of spans to train the model

After the model has been successfully trained according to the parameters, the sampler starts a gRPC listener which exposes two RPCs. The first is an implementation of the OTLP gRPC interface for receiving traces. As shown in figure 2, this allows Collector to stream new traces into the sampler as they are received from upstream applications and infrastructure. The second RPC provides a streaming endpoint which clients can connect to in order to receive sampled spans, which are provided to the client in their entirety as they were received from Collector. These together along with the core sampler logic essentially form a streaming pipeline of spans, with the OTLP endpoint as the source, the sampler logic as a filter and the client endpoint as a sink.

3.2.4 Processor

As described, the processor serves as a downstream component of the sampler within the SCALE architecture. It is the task of the processor to analyze traces and make the ultimate decision on whether to perform any scaling operations. The processor is configured with a set of rules defined via YAML configuration. These rules associate latency thresholds with scaling actions. An example of this is of the form *scale service A if operation B reaches a latency of X, N times within a given window*. The rules then drive the heuristics based analysis of the distributed traces received from the sampler.

The processor is composed of two main components, the consumer and processor engine. The consumer will initiate a streaming gRPC connection to receive the sampled spans using the Python asyncio version of gRPC. The spans received contain all of the same attributes and meta-data that were also received by the sampler. These spans are somewhat hierarchical, but not organized according to traces, and more so to shared data between spans for compaction purposes. The spans are then dropped into an asyncio queue.

The processor engine will then read these spans from the queue. The spans are iterated over and flattened

into a pandas dataframe. The rule set defined in the configuration file is then applied as precompiled predicates against the dataframe. Any rules whose criteria is a match has their actions folded into a conflated action set. The purpose of conflation is to deduplicate redundant scaling actions. When the analysis is complete the processor will then call the Kubernetes shim to perform the scaling action. In addition to scaling analysis and actions, the processor engine will also continually keep several statistics and trend analytics of inspected spans.

3.2.5 Orchestration Shim

The orchestration shim acts as a layer between the processor and Kubernetes itself. Its purpose is to abstract away the specific details of the Kubernetes API, to provide a more generic scaling interface to the processor. This abstraction model allows for the ability to swap out service orchestration backends, or more realistically to compose multiple backends. This is manifested in the form of an OrchestrationClient interface which provides a stub for scaling a resource, and another for getting the current scale of a resource. The shim is meant to be intentionally light weight, and implementations are called directly within the processor.

3.3 Performance and Overhead

In an autoscaling system which is reacting in real time to a constant influx of observability data, one must take into careful consideration how that system itself is performing. First and foremost it cannot be a detriment to the system it is monitoring and making scaling decisions for. Therefore, in any environment our recommendation is that it be run on its own resources which do not contend with your core application resources.

The amount of data that is ingested from observability sources should also be considered. Tight control should be put around the sampling and filtering of the ingestion. The amount of data ingested should coincide with whatever network allocation is provided to the SCALE environment, the amount of memory provided to the sampler and the amount of compute resources you have provided to the processor for analysis. This can be configured either via tuning parameters of the sampler, or pre-sampling and filtering techniques configured within the OpenTelemetry Collector.

The final consideration should be in the analysis cycle of the processor. If the processor is analyzing too often it can overwhelm the SCALE environment. Worse yet, it can create further undesired performance issues in the application environment, as it is continuously put into a stabilization state due to over-scaling. If the processor is not analyzing enough, then SCALE will be too slow to react to scaling needs and the system may degrade at an increasing rate that becomes more difficult to recover

from. Ideally an upper and lower bound on the analysis cycle should be put in place. If the lower bound cannot be met, then likely it is up to the operator to either increase capacity in the SCALE environment, tune observability ingestion volume or review their processor rule set model for possible optimization.

4 Evaluation

4.1 Overview

To evaluate our system, we will create a comprehensive testing environment that simulates real-world traffic patterns, bottlenecks, and resource constraints. This setup will allow for controlled comparisons between baseline autoscaling (CPU/memory-based) and SCALE. We will evaluate the autoscaling systems using open-source benchmarking suites, along with an in-house architecture resembling a personal finance application. To simulate production-like environments, we will use additional open-source simulation tools and chaos testing tools to generate realistic traffic surges and failure conditions across microservices. Our goal is to measure the speed and accuracy of autoscaling decisions made by the observability-driven system compared to the baseline.

4.2 Environment Setup

For our testing we have setup a Kubernetes environment using Minikube⁵, which allows us to spin up full fledged Kubernetes clusters on a single physical node. The server environment is a single 24 core 13th Gen Intel(R) Core(TM) i7-13700F, with 64GiB of dual channel DDR4 main memory. CPU and memory resources allotted to Minikube are configurable, with defaults of 2 virtual cores and 2GiB of memory. We tune these levels, typically increasing them depending on the particular experiment. For test clusters, we are currently utilizing the open-source Online Boutique⁶ benchmark as well as a custom built suite which simulates a financial planning application. As experimentation progresses we will likely explore further open-source benchmarks. For visualizing and examining trace data at rest in Tempo, we are deploying and using Grafana⁷.

4.3 Sampler Evaluation

4.3.1 Parameter Tuning

The performance of the proposed sampling mechanism was optimized by tuning critical parameters to achieve a balance across four key metrics:

False Positive Rate (FPR) FPR measures the proportion of normal spans that are incorrectly flagged as anomalous. This metric is critical for reducing noise in the system. It is calculated as follows:

$$FP = \text{Span incorrectly flagged as anomalous} \quad (1)$$

$$FPR = \frac{FP_{total}}{TotalSpans} \quad (2)$$

Accuracy Accuracy quantifies the proportion of correctly classified spans, encompassing both true positives (TP) and true negatives (TN), relative to the total number of spans. Ensuring 100% accuracy was prioritized to avoid misclassification of both normal and anomalous spans. Accuracy is defined as

$$Accuracy = \frac{(TP + TN)}{TotalSpans} \quad (3)$$

Processing Time Per Span This metric reflects the computational efficiency of the sampler by averaging the time required to process each span. Reducing the value is critical to ensure scalability in high-throughput environments. It is calculated as:

$$T_{span} = \frac{T_{total}}{TotalSpans} \quad (4)$$

F1 Score The F1 Score provides a balanced measure of the sampler's precision and recall, capturing the trade-off between correctly identifying anomalies and minimizing false positives. It's formulated as follows:

$$Precision = \frac{TP}{TP + FP} \quad (5)$$

$$Recall = \frac{TP}{TP + FN} \quad (6)$$

$$F1 = \frac{2 * Precision * Recall}{Precision + Recall} \quad (7)$$

The tuning process involved systematic adjustments of parameters such as the target anomaly score, feature scaling factors, height, number of trees, and window size. Each iteration was evaluated against the aforementioned metrics with the goal of minimizing FPR, maintaining 100% detection accuracy, reducing processing time, and maximizing the F1 score. These adjustments were guided by a feedback loop, enabling continuous improvement to optimize sampler performance.

The Parallel Coordinate Plot in figure 3 shows the parameter tuning process aimed at reducing the False Positive Rate, which ultimately converged on a parameter set with an optimized FPR at 1.982.

⁵<https://minikube.sigs.k8s.io/>

⁶<https://github.com/Mark-McCracken/online-boutique>

⁷<https://grafana.com/>

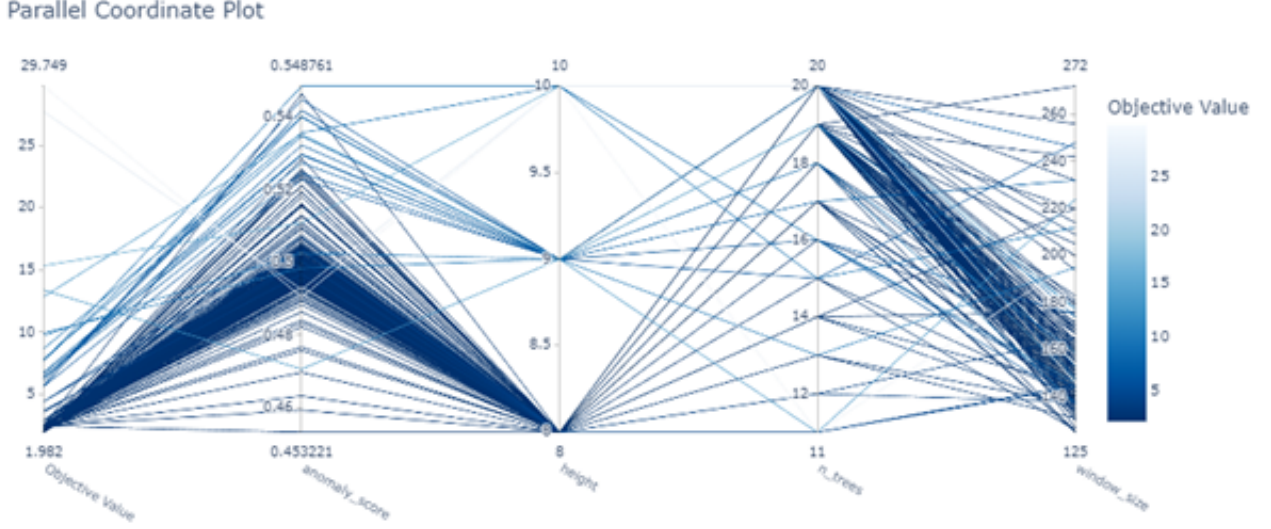


Figure 3: Parameter Tuning Plot

4.3.2 Dataset Analysis

The optimized sampler evaluated against two datasets used in previous studies (*GTrace* [15] and *TraceMesh* [5]). For both datasets, the sampler was benchmarked on the following metrics: precision, recall, F1 score, processing time, and FPR. Results demonstrated the sampler consistently maintained 100% accuracy, minimized FPR, and delivered competitive F1 scores while adhering to stringent efficiency requirements. Table 2 shows the results of these experiments.

Table 2: Dataset Comparison

Metric	GTrace	TraceMesh
Total Spans	4881687	57908
Anomalies Detected	196987	4344
True Positives	81361	2895
False Positives	115626	1449
False Negatives	0	0
Precision	0.41302726	0.66643646
Recall	1.0	1.0
F1 Score	0.58459913	0.79983423
Processing Time	71 μ s	77 μ s

Figures 4 and 5 present confusion matrices which detail how well the model compared vs. expected results.

Figures 6 and 7 present violin plots which show the scoring density of normal vs. anomalous spans.

4.4 Processor Evaluation

The processor’s work is of deterministic nature, and thus unlike the sampler doesn’t have a measurable fitness. The

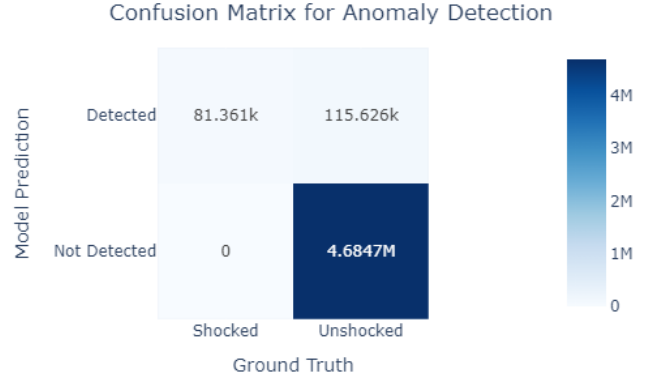


Figure 4: GTrace Dataset Confusion Matrix

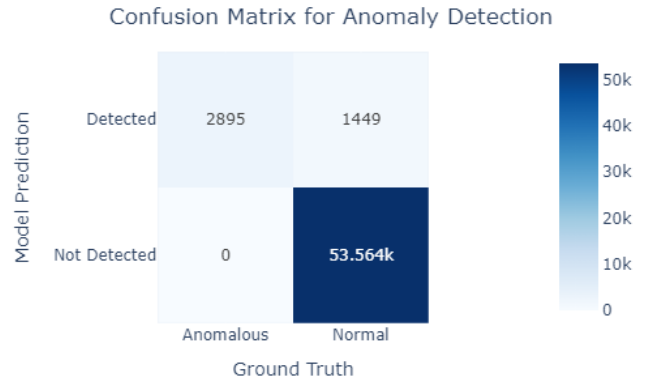


Figure 5: TraceMesh Dataset Confusion Matrix

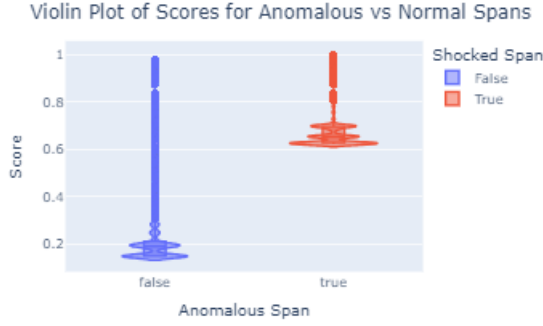


Figure 6: GTrace Scoring

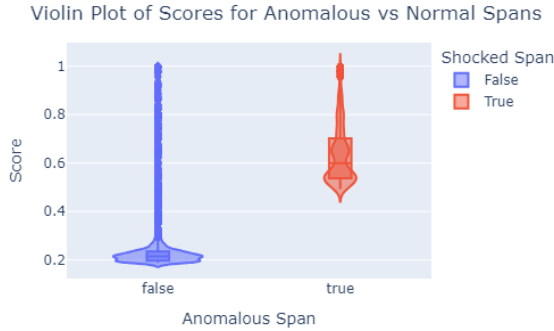


Figure 7: TraceMesh Scoring

general functionality of the processor can therefore be easily tested via straightforward unit and integration testing. These characteristics aside, quantifiable aspects of the processor which are of pertinent interest include capacity and throughput metrics. While the sampler’s job is to reduce the spans seen by the processor to those deemed anomalous there will no doubt be some level of false positives. In larger distributed systems, these false positives and even valid anomalies can equate to significant traffic. We stress tested and recorded measurements to ensure the processor can handle moderately sized loads.

4.4.1 Memory Footprint

The first of the metrics we tested for the processor is the space needed to queue the spans in memory. To test this we used two sets of data both generated by otelgen. The first was with it’s mobile_web scenario and the second with it’s microservices scenario. With mobile_web the traces are small, consisting of only a single span. The microservices scenario however has on average about 100 spans. Traces are streamed in and stored in memory as open telemetry compliant protocol buffers. For each scenario we streamed 2000 traces. Table 3 shows what the size in memory came out to in our experimentation.

Table 3: Span Memory Footprint (2000 Traces)

Scenario	Size (bytes)
mobile_web	11395204
microservices	94141443

We can see that with mobile_web there was minimal in size at ~11MB. With microservices we see that this jumps to ~100MB. However, even for heavier loads in the tens of thousands, we are only talking about a handful of gigabytes, something quite manageable by today’s memory standards. We also notice that there is a large gain in grouping of like span data, as a trace for microservices has 100 as many spans, but only 10 times the memory footprint.

4.4.2 Span Analysis Throughput

Arguably much more important than the memory footprint of queued traces is the speed at which the processor engine can iterate through sampled traces that have been placed into it’s queue by the span consumer. To simulate heavy load, we ran 3 different tests, each with a different flavor of trace data. The first with mobile_web traces from otelgen, the second with microservices traces from otelgen and finally the last with traces from the online boutique benchmark. Each test instantiates a processor with a mocked orchestration shim, queries 20000 traces from Tempo, and executes the processing stage. The results of these runs can be seen in Table 4.

Table 4: Processor Trace Throughput

Scenario	Time per 20000 Traces
mobile_web	0.232s
microservices	56.805s
online boutique	3.615s

Based on the known number of spans per trace, the mobile_web run comes out to around 86k spans per second, and the microservices comes out to about 35k spans per second. The extra overhead of the microservices traces can be attributed to their depth and large attribute footprint. For the online boutique, spans per trace are random, but span attribute complexity is similar to that of microservices. With this information, if we assume a sampling rate even as high as 5%, the processor should be able to handle a distributed system that is generating well over half a million spans per second.

References

- [1] M. Straesser, J. Grohmann, J. von Kistowski, S. Eismann, A. Bauer, S. Kounev, Why is it not solved yet? Challenges for production-ready autoscaling, in: Proceedings of the 2022 ACM/SPEC on International Conference on Performance Engineering, Association for Computing Machinery, New York, NY, USA, 2022: pp. 105–115. <https://doi.org/10.1145/3489525.3511680>⁸.
- [2] C. Eder, S. Winzinger, R. Lichtenthaler, A comparison of distributed tracing tools in serverless applications, in: 2023 IEEE International Conference on Service-Oriented System Engineering (SOSE), IEEE Computer Society, Los Alamitos, CA, USA, 2023: pp. 98–105. <https://doi.org/10.1109/SOSE58276.2023.00018>⁹.
- [3] G. Yu, P. Chen, Z. Zheng, Microscaler: Automatic scaling for microservices with an online learning approach, in: 2019 IEEE International Conference on Web Services (ICWS), 2019: pp. 68–75. <https://doi.org/10.1109/ICWS.2019.00023>¹⁰.
- [4] T.-T. Nguyen, Y.-J. Yeom, T. Kim, D.-H. Park, S. Kim, Horizontal pod autoscaling in kubernetes for elastic container orchestration, *Sensors* 20 (2020). <https://doi.org/10.3390/s20164621>¹¹.
- [5] Z. Chen, Z. Jiang, Y. Su, M.R. Lyu, Z. Zheng, Tracemesh: Scalable and Streaming Sampling for Distributed Computing Systems Workshops (ICDCSW), title=Towards a lightweight distributed telemetry for microservices, year=2024, volume=, number=, pages=75-82, keywords=Root cause analysis;Biological system modeling;System performance;Ecosystems;Microservice architectures;Computer architecture;User interfaces;telemetry;oas;api;microservices, doi=10.1109/ICDCSW63686.2024.00018, in: 2024 IEEE 17th International Conference on Cloud Computing (CLOUD), IEEE Computer Society, Los Alamitos, CA, USA, 2024: pp. 54–65. <https://doi.org/10.1109/CLOUD62652.2024.00016>¹².
- [6] E. Manzoor, S.M. Milajerdi, L. Akoglu, Fast memory-efficient anomaly detection in streaming heterogeneous graphs, in: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Association for Computing Machinery, New York, NY, USA, 2016: pp. 1035–1044. <https://doi.org/10.1145/2939672.2939783>¹³.
- [7] F. Cao, M. Estert, W. Qian, A. Zhou, Density-based clustering over an evolving data stream with noise, in: Proceedings of the 2006 SIAM International Conference on Data Mining (SDM), 2006: pp. 328–339. <https://doi.org/10.1137/1.9781611972764.29>¹⁴.
- [8] H. Qiu, S.S. Banerjee, S. Jha, Z.T. Kalbarczyk, R.K. Iyer, FIRM: An intelligent fine-grained resource management framework for SLO-Oriented microservices, in: 14th USENIX Symposium on Operating Systems Design and Implementation (OSDI 20), USENIX Association, 2020: pp. 805–825. <https://www.usenix.org/conference/osdi20/presentation/qiu>.
- [9] H. Qiu, W. Mao, C. Wang, H. Franke, A. Youssef, Z.T. Kalbarczyk, T. Başar, R.K. Iyer, AWARE: Automate workload autoscaling with reinforcement learning in production cloud systems, in: 2023 USENIX Annual Technical Conference (USENIX ATC 23), USENIX Association, Boston, MA, 2023: pp. 387–402. <https://www.usenix.org/conference/atc23/presentation/qiu-haoran>.
- [10] S. Luo, H. Xu, K. Ye, G. Xu, L. Zhang, G. Yang, C. Xu, The power of prediction: Microservice auto scaling via workload learning, in: Proceedings of the 13th Symposium on Cloud Computing, Association for Computing Machinery, New York, NY, USA, 2022: pp. 355–369. <https://doi.org/10.1145/3542929.3563477>¹⁵.
- [11] G. Christofidi, K. Papaioannou, T.D. Doudali, Is machine learning necessary for cloud resource usage forecasting?, in: Proceedings of the 2023 ACM Symposium on Cloud Computing, Association for Computing Machinery, New York, NY, USA, 2023: pp. 544–554. <https://doi.org/10.1145/3620678.3624790>¹⁶.
- [12] OpenTelemetry, OpenTelemetry, (2024). <https://opentelemetry.io/> (accessed October 25, 2024).
- [13] Grafana, Grafana tempo OSS: Distributed tracing backend, (2024). <https://grafana.com/oss/tempo/> (accessed October 25, 2024).
- [14] S.C. Tan, K.M. Ting, T.F. Liu, Fast anomaly detection for streaming data, in: Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence - Volume Volume Two, AAAI Press, Barcelona, Catalonia, Spain, 2011: pp. 1511–1516.

- [15] Z. Xie, C. Pei, W. Li, H. Jiang, L. Su, J. Li, G. Xie, D. Pei, From point-wise to group-wise: A fast and accurate microservice trace anomaly detection approach, in: *Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, Association for Computing Machinery, New York, NY, USA, 2023: pp. 1739–1749. <https://doi.org/10.1145/3611643.3613861>¹⁷.
- [16] S. Luo, H. Xu, C. Lu, K. Ye, G. Xu, L. Zhang, Y. Ding, J. He, C. Xu, Characterizing microservice dependency and performance: Alibaba trace analysis, in: *Proceedings of the ACM Symposium on Cloud Computing*, Association for Computing Machinery, New York, NY, USA, 2021: pp. 412–426. <https://doi.org/10.1145/3472883.3487003>¹⁸.
- [17] J. Shen, H. Zhang, Y. Xiang, X. Shi, X. Li, Y. Shen, Z. Zhang, Y. Wu, X. Yin, J. Wang, M. Xu, Y. Li, J. Yin, J. Song, Z. Li, R. Nie, Network-centric distributed tracing with DeepFlow: Troubleshooting your microservices in zero code, in: *Proceedings of the ACM SIGCOMM 2023 Conference*, Association for Computing Machinery, New York, NY, USA, 2023: pp. 420–437. <https://doi.org/10.1145/3603269.3604823>¹⁹.
- [18] D. Cha, Y. Kim, Service mesh based distributed tracing system, in: *2021 International Conference on Information and Communication Technology Convergence (ICTC)*, 2021: pp. 1464–1466. <https://doi.org/10.1109/ICTC52510.2021.9620968>²⁰.
- [19] S. Ashok, V. Harsh, B. Godfrey, R. Mittal, S. Parthasarathy, L. Shwartz, TraceWeaver: Distributed request tracing for microservices without application modification, in: *Proceedings of the ACM SIGCOMM 2024 Conference*, Association for Computing Machinery, New York, NY, USA, 2024: pp. 828–842. <https://doi.org/10.1145/3651890.3672254>²¹.
- [20] M. Toslali, S. Qasim, S. Parthasarathy, F.A. Oliveira, H. Huang, G. Stringhini, Z. Liu, A.K. Coskun, An online probabilistic distributed tracing system, (2024). <https://arxiv.org/abs/2405.15645>.
- [21] Y. Zhang, R. Isaacs, Y. Yue, J. Yang, L. Zhang, Y. Vigfusson, LatenSeer: Causal modeling of end-to-end latency distributions by harnessing distributed tracing, in: *Proceedings of the 2023 ACM Symposium on Cloud Computing*, Association for Computing Machinery, New York, NY, USA, 2023: pp. 502–519. <https://doi.org/10.1145/3620678.3624787>²².
- [22] H. Huang, X. Zhang, P. Chen, Z. He, Z. Chen, G. Yu, H. Chen, C. Sun, TraStrainer: Adaptive sampling for distributed traces with system runtime state, *Proc. ACM Softw. Eng.* 1 (2024). <https://doi.org/10.1145/3643748>²³.
- [23] S. He, B. Feng, L. Li, X. Zhang, Y. Kang, Q. Lin, S. Rajmohan, D. Zhang, STEAM: Observability-preserving trace sampling, in: *Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, Association for Computing Machinery, New York, NY, USA, 2023: pp. 1750–1761. <https://doi.org/10.1145/3611643.3613881>²⁴.
- [24] V. Sachidananda, A. Sivaraman, Erlang: Application-aware autoscaling for cloud microservices, in: *Proceedings of the Nineteenth European Conference on Computer Systems*, Association for Computing Machinery, New York, NY, USA, 2024: pp. 888–923. <https://doi.org/10.1145/3627703.3650084>²⁵.
- [25] J. Liu, Q. Wang, S. Zhang, L. Hu, D. Da Silva, Sora: A latency sensitive approach for microservice soft resource adaptation, in: *Proceedings of the 24th International Middleware Conference*, Association for Computing Machinery, New York, NY, USA, 2023: pp. 43–56. <https://doi.org/10.1145/3590140.3592851>²⁶.
- [26] M. Fourati, S. Marzouk, M. Jmaiel, Towards microservices-aware autoscaling: A review, in: *2023 IEEE Symposium on Computers and Communications (ISCC)*, IEEE Computer Society, Los Alamitos, CA, USA, 2023: pp. 1080–1083. <https://doi.org/10.1109/ISCC58397.2023.10218213>²⁷.
- [27] P. Las-Casas, G. Papakerashvili, V. Anand, J. Mace, Sifter: Scalable sampling for distributed traces, without feature engineering, in: *Proceedings of the ACM Symposium on Cloud Computing*, Association for Computing Machinery, New York, NY, USA, 2019: pp. 312–324. <https://doi.org/10.1145/3357223.3362736>²⁸.
- [28] Z. Huang, P. Chen, G. Yu, H. Chen, Z. Zheng, Sieve: Attention-based sampling of end-to-end trace data in distributed microservice systems, in: *2021 IEEE International Conference on Web Services (ICWS)*, 2021: pp. 436–446. <https://doi.org/10.1109/ICWS53863.2021.00063>²⁹.

- [29] E. Manzoor, S.M. Milajerdi, L. Akoglu, Fast memory-efficient anomaly detection in streaming heterogeneous graphs, in: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Association for Computing Machinery, New York, NY, USA, 2016: pp. 1035–1044. <https://doi.org/10.1145/2939672.2939783>³⁰.
- [30] M. Otero, J.M. Garcia, P. Fernandez, Towards a lightweight distributed telemetry for microservices, in: 2024 IEEE 44th International Conference on Distributed Computing Systems Workshops (ICDCSW), 2024: pp. 75–82. <https://doi.org/10.1109/ICDCSW63686.2024.00018>³¹.
- [31] G. Yu, P. Chen, Y. Li, H. Chen, X. Li, Z. Zheng, Nezha: Interpretable fine-grained root causes analysis for microservices on multi-modal observability data, in: Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, Association for Computing Machinery, New York, NY, USA, 2023: pp. 553–565. <https://doi.org/10.1145/3611643.3616249>³².
- [32] A. Belkhiri, M. Ben Attia, F. Gohring De Magalhaes, G. Nicolescu, Towards efficient diagnosis of performance bottlenecks in microservice-based applications (work in progress paper), in: Companion of the 15th ACM/SPEC International Conference on Performance Engineering, Association for Computing Machinery, New York, NY, USA, 2024: pp. 40–46. <https://doi.org/10.1145/3629527.3651432>³³.
- [33] A. Belkhiri, A. Shahnejat Bushehri, F. Gohring de Magalhaes, G. Nicolescu, Transparent trace annotation for performance debugging in microservice-oriented systems (work in progress paper), in: Companion of the 2023 ACM/SPEC International Conference on Performance Engineering, Association for Computing Machinery, New York, NY, USA, 2023: pp. 25–32. <https://doi.org/10.1145/3578245.3585030>³⁴.
- [34] L. Huang, T. Zhu, Tprof: Performance profiling via structural aggregation and automated analysis of distributed systems traces, in: Proceedings of the ACM Symposium on Cloud Computing, Association for Computing Machinery, New York, NY, USA, 2021: pp. 76–91. <https://doi.org/10.1145/3472883.3486994>³⁵.
- [35] Minikube, Minikube, (2024). <https://minikube.sigs.k8s.io/> (accessed October 26, 2024).
- [36] River, River, (2024). <https://riverml.xyz/dev/> (accessed November 15, 2024).
- [37] P. Las-Casas, J. Mace, D. Guedes, R. Fonseca, Weighted sampling of execution traces: Capturing more needles and less hay, in: Proceedings of the ACM Symposium on Cloud Computing, Association for Computing Machinery, New York, NY, USA, 2018: pp. 326–332. <https://doi.org/10.1145/3267809.3267841>³⁶.
- [38] S. Bhatia, M. Wadhwa, K. Kawaguchi, N. Shah, P.S. Yu, B. Hooi, Sketch-based anomaly detection in streaming graphs, in: Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, Association for Computing Machinery, New York, NY, USA, 2023: pp. 93–104. <https://doi.org/10.1145/3580305.3599504>³⁷.
- [39] P. Liu, H. Xu, Q. Ouyang, R. Jiao, Z. Chen, S. Zhang, J. Yang, L. Mo, J. Zeng, W. Xue, D. Pei, Unsupervised detection of microservice trace anomalies through service-level deep bayesian networks, in: 2020 IEEE 31st International Symposium on Software Reliability Engineering (ISSRE), 2020: pp. 48–58. <https://doi.org/10.1109/ISSRE5003.2020.00014>³⁸.

Appendix

Code Repository

Current works are hosted at our Illinois GitLab Repository at <https://gitlab.engr.illinois.edu/cs598-ccc-jkss/cs598-project>. We are tracking feature and documentation tasks, as well as bugs in the issues section of the repository.