

# MICRORACER: Detecting Concurrency Bugs for Cloud Service Systems

Zhiling Deng  
Sun Yat-sen University  
Zhuhai, China  
dengzhiling3@mail2.sysu.edu.cn

Juepeng Wang  
Sun Yat-sen University  
Zhuhai, China  
wangjp39@mail2.sysu.edu.cn

Zhuangbin Chen<sup>†</sup>  
Sun Yat-sen University  
Zhuhai, China  
chenzhib36@mail.sysu.edu.cn

**Abstract**—Modern cloud applications delivering global services are often built on distributed systems with a microservice architecture. In such systems, end-to-end user requests traverse multiple different services and machines, exhibiting intricate interactions. Consequently, cloud service systems are vulnerable to *concurrency bugs*, which pose significant challenges to their reliability. Existing methods for concurrency bug detection often fall short due to their intrusive nature and inability to handle the architectural complexities of microservices. To address these limitations, we propose MICRORACER, a non-intrusive and automated framework for detecting concurrency bugs in such environments. By dynamically instrumenting widely-used libraries at runtime, MICRORACER collects detailed trace data without modifying the application code. Such data are utilized to analyze the happened-before relationship and resource access patterns of common operations within service systems. Based on this information, MICRORACER identifies suspicious concurrent operations and employs a three-stage validation process to test and confirm concurrency bugs. Experiments on open-source microservice benchmarks with replicated industrial bugs demonstrate MICRORACER’s effectiveness and efficiency in accurately detecting and pinpointing concurrency issues.

**Index Terms**—Concurrency bugs, Microservices, Cloud service reliability, Distributed tracing

## I. INTRODUCTION

Cloud service systems, characterized by their distributed nature and microservice architecture, offer unparalleled scalability and flexibility. This architectural approach empowers businesses to innovate rapidly and deliver superior user experiences. For instance, Uber operates with several thousand microservices [1], enabling it to efficiently provide seamless services across different regions. Similarly, WeChat hosts over 3,000 microservices to handle billions of daily requests worldwide [2]. With this level of complexity and scale, ensuring the reliability of cloud service systems becomes paramount [3].

In such systems, the end-to-end request flows are inherently complex, involving interactions among multi-tier services and machines. Due to the large number of simultaneous execution of multiple operations, cloud service systems often suffer from *concurrency bugs* [3], [4], which could lead to inconsistent states, data corruption, and ultimately system failures. Modern cloud services typically employ a loosely coupled design, with each maintaining its own independent datastore [5]. A single user request can make multiple read and write operations

across different datastores (owned by different services) during the course of its execution. This further compounds the complexity to managing data consistency and system reliability.

Concurrency bug detection is a well-studied topic in distributed systems [6], [7] and web applications [5], [8], [9]. However, traditional distributed systems, such as Hadoop and Zookeeper, typically do not involve independent datastores for each component. Meanwhile, race detection in web applications addresses the issue from the perspective of external client requests, often neglecting the internal complexities and architectural characteristics of cloud service systems. As a result, existing methods fail to consider these unique architectural aspects, rendering them less effective in the context of microservice environments. Moreover, these tools are often intrusive [10], [11]. They instrument application source code to monitor and control execution, which can introduce significant overhead and potentially alter the behavior of the system being analyzed. Therefore, there is a pressing need for non-intrusive and effective techniques tailored to the specific challenges posed by microservice architectures in cloud service systems. We introduce the primary challenges as follows:

- **Complex Communication Patterns:** Microservice systems involve a variety of communication patterns, such as request-response, event-driven, and message queues. This introduces non-deterministic execution orders and complicated timing relationships that are difficult to reason about. Standard happen-before models [9], [12] may not be sufficient to capture these complex, application-level communication semantics, making it challenging to accurately determine which operations are truly concurrent.
- **Decentralized State and Cross-service Inconsistency:** Microservices promote a “database-per-service” design, resulting in multiple independent and “mutually-oblivious” datastores [5]. A single end-user request often runs across several services, performing writes to these different datastores. This creates an implicit causal dependency across services that traditional consistency models, which operate within a single datastore, cannot see or enforce.
- **Accuracy and Automation in Bug Validation:** An effective concurrency bug detection method must be able to achieve high accuracy in identifying concurrency issues, minimizing both false positives and false negatives. More-

<sup>†</sup>Zhuangbin Chen is the corresponding author.

over, the bug validation process should be automated to reduce the need for extensive human intervention, such as writing assertions manually to check the correctness of system behaviors [13]–[15].

To address these challenges, we propose MICRO-RACER in this work, a concurrency bug detection framework for microservice systems, which is non-intrusive and automated. At a high level, MICRO-RACER achieves this goal by first identifying suspicious pairs of concurrent operations based on trace analysis, and subsequently testing for concurrency issues by reversing their execution order. If reversing the order leads to different results or errors, it indicates the presence of potential concurrency bugs.

MICRO-RACER tackles the first challenge by employing dynamic instrumentation to automatically instrument widely-used libraries at runtime, rather than modifying the application’s code. We focus on the libraries for common operations in cloud services, such as request/response handling, database interactions, message queuing, among others. This approach facilitates the collection of trace data, which capture the happened-before relationship of these operations and their resource access patterns. Based on such information, MICRO-RACER analyzes concurrent behaviors between different microservices and identifies potential issues. For the second challenge, MICRO-RACER carefully examines the resource access patterns among different request flows. Only pairs that access the same resource entities with at least one write operation will be selected. We also employ pruning strategies to narrow down the search space by considering both shared state locality and the causal dependencies in a request flow. To address the last challenge, MICRO-RACER executes a three-stage validation process to automatically ascertain whether a pair of concurrent operations triggers a bug. Particularly, to accelerate this process, MICRO-RACER performs an early validation to preliminarily uncover pairs with obvious conflicts.

We demonstrate the practical effectiveness of MICRO-RACER through experiments with 14 industrial concurrency bugs replicated on four open-source microservice benchmarks, i.e., TrainTicket [16], Bank of Anthos [17], and two applications from DeathStarBench [18]. Our evaluation shows that MICRO-RACER is able to accurately identify concurrent operations in microservices and effectively pinpoint bugs.

To sum up, we make the following major contributions:

- We propose MICRO-RACER, a non-intrusive framework for automated concurrency bug detection in microservice systems. MICRO-RACER instruments widely-used libraries to monitor the happened-before relationship among common service operations and their resource access patterns. It then locates the suspicious concurrent operations and validates their correctness by controlling their execution order.
- We conduct experiments with popular open-source microservices benchmarks, where we replicate industrial bug cases. The experimental results demonstrate the efficiency and effectiveness of MICRO-RACER in revealing concurrency bugs in microservices systems. The imple-

mentation of MICRO-RACER and bug replications are publicly available<sup>1</sup>.

## II. BACKGROUND

### A. Concurrency Issues in Cloud Services

Cloud service systems predominantly adopt architectural patterns that emphasize the loose coupling of services. Each service can handle requests independently, enabling the system to distribute the load and process multiple requests in parallel. In such systems, the execution flows of user requests often involve complex interactions among multiple services. As a result, concurrency issues can arise, posing significant threats to system reliability and performance.

Compared to traditional distributed systems and web applications, concurrency issues in cloud service systems are exacerbated by several factors. First, the microservices architecture, which promotes independent databases and network-based communication among services, introduces challenges such as inconsistent states, partial failures, and intricate dependency chains. The fact that cloud services may span multiple data centers or even regions further complicates matters with network latency, partitioning, and synchronization issues. Moreover, many cloud services adopt eventual consistency models to enhance performance and scalability, leading to scenarios where different parts of the system hold divergent views of the data. This inconsistency can cause concurrency issues when services interact. Asynchronous communication mechanisms, such as message queues and event streams, introduce non-deterministic execution orders and timing challenges, adding another layer of complexity.

Therefore, to detect concurrency bugs in such systems, we must be able to effectively monitor the key points of interaction between services to log relevant states and events, such as database accesses, message queue operations, and inter-service communications. These data serve as the basis for identifying patterns and anomalies that indicate potential concurrency issues.

### B. Distributed Tracing

As discussed in Sec. II-A, the complexity of inter-service communication and the dynamic nature of microservices architecture require robust mechanisms for observability and monitoring. One such mechanism is distributed tracing, which plays a pivotal role in understanding the behavior and performance of distributed applications [19]–[23]. A trace is a structured record that captures the hierarchical sequence of events that occur in multiple nodes or components, forming a tree-like representation of the request’s journey through the system [24], [25]. It is composed of multiple spans, which are the basic units of work that represent a single, indivisible operation within a service. Each span includes critical information such as timestamps, service logs, and identifiers that link it to other spans within the same trace.

<sup>1</sup><https://github.com/OpsPAI/MicroRacer>

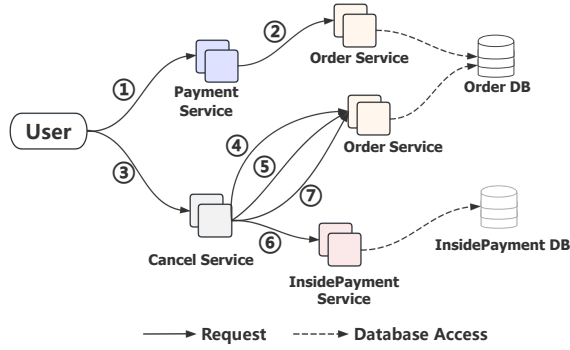


Fig. 1. Service call graph of the illustrating example

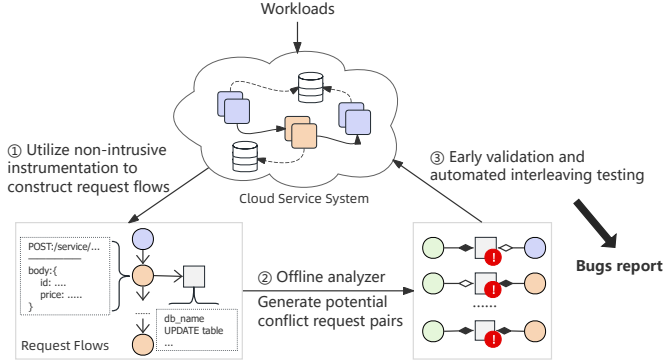


Fig. 2. The architecture of MICRORACER

The concept of tracing has been extensively employed to understand system behavior, particularly for reliability analysis [26] and performance bottleneck identification [27], [28]. For instance, [8], [9], [11], [12] have leveraged distributed tracing to detect and resolve concurrency issues, based on static and dynamic analysis techniques. In these works, static analysis involves injecting tracing logic into the application code to collect state data, which helps identify potential concurrency issues by examining the code structure and execution paths; while dynamic analysis requires specifying operations such as thread-related activities, RPC interfaces, and socket communication for tracing, allowing for real-time monitoring and capturing of the system’s behavior under various load conditions. Therefore, they often necessitate manual instrumentation, which is intrusive and ad-hoc, thereby limiting the generalizability and completeness of the collected data.

In this work, we explore a unified approach of distributed tracing that is non-intrusive to the application. By employing bytecode-level instrumentation, we intercept calls to common libraries used by applications and inject tracing code dynamically. The traces are then used to construct requests flows that reflect the architecture of microservices. This method allows for the collection of traces without modifying the application code and enhances the detection of concurrency bugs.

### C. An Illustrating Example

In this section, we present an example of concurrency bug, which is a functional fault reported by an industrial sur-

vey [16]. The bug has been replicated in the TrainTicket [29], a widely-used benchmark in microservice-related research.

Fig. 1 depicts the service call graph for this bug, which originates from a race condition between two user-initiated operations, i.e., a payment and a subsequent cancellation for the same order. From the perspective of our framework, these actions trigger two distinct, concurrently executing request flows, i.e., flow A (payment): ①→② and flow B (cancellation): ③→④→⑤→⑥→⑦. The core flaw lies in the system’s optimistic assumption that the payment flow (A) will always complete before the cancellation flow (B) begins. However, in a distributed environment, factors like network latency and service scheduling make execution order non-deterministic. This creates a race where both flows compete to read and write to the same order entity in the Order DB. Let us trace the intended and the buggy execution flows:

- **Initial State:** The order exists in the Order DB with a status of 0 (Not Paid).
- **Intended (Sequential) Execution:** The Payment Service would process the request, calling the Order Service (②) to update the order status to Paid. Subsequently, the Cancel Service would handle request ③, read the Paid status, and correctly initiate a refund.
- **Buggy (Concurrent) Execution:** Due to non-deterministic factors like network latency, the cancellation flow begins before the payment flow completes. The Cancel Service invokes the Order Service (④), which reads the order’s state. Because the payment is still pending, it retrieves the stale status Not Paid. Based on this outdated information, the Cancel Service’s business logic incorrectly concludes that no refund is required. It then proceeds with the cancellation, updating the order status first to 7 (Refunding) via request ⑤ and finally to 4 (Cancelled) via request ⑦. Concurrently, the Payment Service eventually processes request ②, successfully charging the user and updating the order in the database.

The result is a critical data consistency failure: the user is charged for the order, but the system fails to issue a refund because the cancellation logic operated on stale data. The fault appears to be a classic server-side request race, but its root cause is deeper, originating from the distributed nature of the architecture. The conflict is an inter-service race condition, where multiple services (Payment Service, Cancel Service) concurrently access and modify a shared resource (the order entity) managed by another service (Order Service). This scenario highlights the difficulty of maintaining correctness when state transitions are coordinated across independent, “mutually-oblivious” services, a primary challenge MICRO-RACER is designed to detect.

## III. METHODOLOGY

### A. Overview

To detect concurrency bugs in service systems similar to those implied in Fig. 1, we propose MICRORACER, a framework that tracks request flows in cloud service systems based

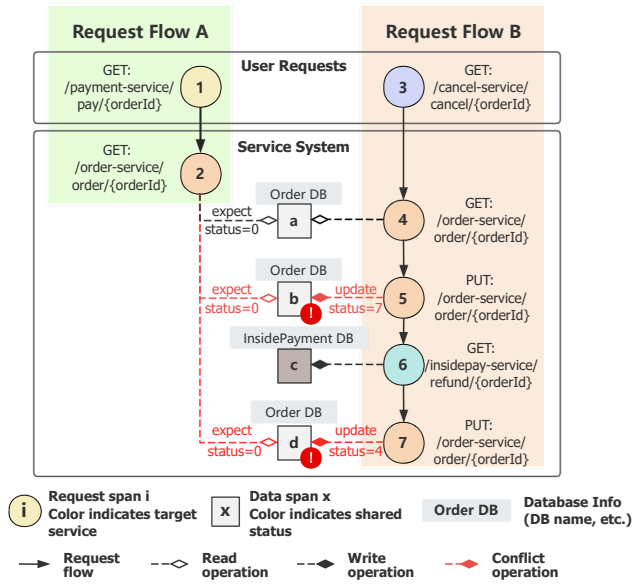


Fig. 3. Request flows of the illustrating example. The flow A (1→2) and the flow B (3→4→5→6→7) have race conditions at data spans b and d.

on non-intrusive instrumentation and automates the detection of request concurrency bugs. The architecture of MICRO-RACER is shown in Fig. 2, which consists of three phases, i.e., *request flow tracing*, *conflict request pair identification*, and *automated bug validation*.

The first phase uses non-intrusive instrumentation to capture end-to-end request flows as the system executes workloads. This process records detailed traces of inter-service calls and operations on shared state resources (e.g., databases, caches). The second phase processes these traces to link requests to the specific data entities they access. It then identifies potential conflicts, i.e., pairs of requests that access the same entity where at least one is a write operation. To improve efficiency, we apply static pruning strategies based on state store locality and request flow causality to significantly narrow the search space. The final phase confirms true positives. It first performs a fast-pass early validation for obvious bugs. The remaining suspicious pairs then undergo automated interleaving testing, where the requests are replayed in both original and reversed orders. A bug is confirmed if this reordering produces a different outcome, as verified by a testing oracle.

### B. End-to-end Request Flow Construction

To detect concurrency bugs, MICRO-RACER must understand the interactions between services and their access to shared states. This is achieved by recording inter-service calls (e.g., via REST APIs, RPC, or message queues) and operations on shared state resources (e.g., databases, caches, object stores) at runtime. From these data, it builds end-to-end request flows that link the original user requests to the specific stateful operations they trigger. These detailed traces are fundamental for identifying potential conflicting request pairs and corresponding test cases, which are crucial for

helping developers find the root cause of the bugs reported by MICRO-RACER.

MICRO-RACER records two types of runtime information, i.e., *data span* and *request span*. When the system receives a user request, MICRO-RACER assigns it a unique flow ID. This flow ID is propagated across service calls, linking individual request spans into a coherent request flow. A data span represents a single, atomic operation on a shared state resource. Each request span can be associated with one or more data spans, depending on how many times the service accesses shared states. Consequently, a request flow starts with a user request and chains together the sequence of inter-service calls and shared state interactions, as illustrated in Fig. 3.

1) *Instrumentation for Data Span*: To record operations on shared state, MICRO-RACER instruments different client libraries and SDKs used to interact with various state stores. This approach captures a complete picture of the potential conflicts in modern microservice systems. A data span is created for each interaction, tagged with the propagated flow context to link it back to the originating request.

- **Databases**: For traditional databases, we instrument commonly-used interfaces like JDBC. MICRO-RACER records the database connection information and the full SQL statement, which are used to infer the specific database entities being accessed (e.g., by parsing the primary keys from WHERE clauses).
- **Message Queues**: For message queue systems such as Kafka and RabbitMQ, MICRO-RACER instruments the producer and consumer client libraries. It captures the topic/queue name, partition key, and relevant message headers or payload identifiers. A `produce` operation is treated as a write to the shared state (the topic), while a `consume` operation is treated as a read.
- **Caches**: For distributed caches like Redis or Memcached, the instrumentation targets the client APIs. MICRO-RACER records the key being accessed and the type of operation (e.g., GET for a read; SET, DEL for a write).
- **Shared Storage**: For object stores like Amazon S3 or shared file systems, MICRO-RACER instruments the corresponding SDKs. It records the bucket and object key (or file path) as the resource identifier and classifies operations like `getObject` as reads and `putObject` as writes.

By instrumenting these various client libraries, MICRO-RACER creates data spans that associate each state access operation with the correct request flow.

2) *Instrumentation for Request Span*: To trace inter-service communication, MICRO-RACER automatically instruments the library APIs used for various protocols, in contrast to previous studies [30]–[32] based on static analysis. While this section focuses on REST APIs, the same principles apply to other communication protocols like gRPC or asynchronous messaging, which can be traced by instrumenting their respective library APIs. Specifically, when a service makes an REST API call to another, it typically uses standard HTTP client libraries. MICRO-RACER instruments these libraries to record request information (headers, body) before and after the call,

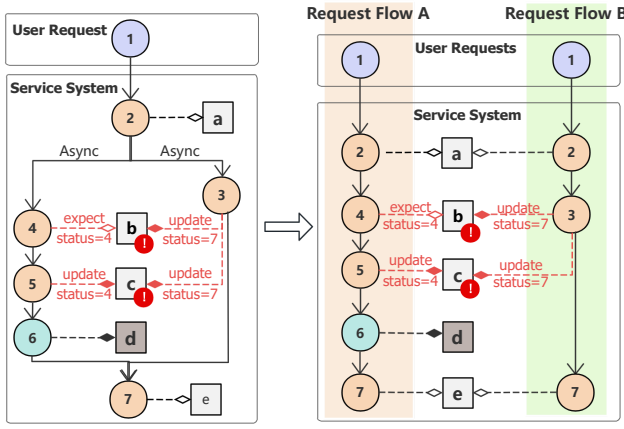


Fig. 4. Request flows when a service asynchronously invokes other services. The left diagram shows the actual request flow in the system, while the right diagram shows the request flow split by MICRORACER during analysis.

forming a request span. To enable cross-service tracing, MICRORACER injects the flow context (containing the flow ID) into the request headers, following standard distributed tracing practices. It also instruments server-side request handlers to receive and maintain this context.

In asynchronous scenarios where a service spawns new threads for parallel processing, MICRORACER instruments common asynchronous frameworks (e.g., Spring Async Annotation). It wraps asynchronous tasks (like `Callable` objects) with the flow context, ensuring that requests initiated from these new threads are correctly associated with the original request flow. A request may diverge when a main thread and sub-threads initiate requests concurrently, and later converge when the main thread waits for the sub-threads to complete. To simplify conflict analysis, we split such complex flows into multiple, sequential request flows. For example, in Fig. 4, the service handling request (2) starts a sub-thread that sends request (3) in parallel with the main thread's requests (4), (5), and (6), then waits for the sub-thread to complete before sending request (7). MICRORACER regards this as two distinct request flows (as shown on the right), allowing it to correctly identify potential conflicts between requests like (3) and (4).

Besides service invocations and intra-request parallelism, MICRORACER also identifies inter-request synchronization through library instrumentation of distributed locks and message queues. For distributed locks, it records the lock identifier and operations (such as `SETNX` in Redis) to determine the mutual exclusion relationship between request flows. For message queues, it links the request flow that sends a message to the request flow that processes it, treating the message passing as a synchronization point. This comprehensive instrumentation enables MICRORACER to accurately model a wide range of common, explicit synchronization patterns, i.e., service calls, internal parallelism, distributed locks, and message queues.

3) *An Example*: Fig. 3 visualizes the output of our request flow construction phase, modeling the bug from the illustrating example (Fig. 1). The two request flows are shown with

distinct background colors. Request spans are represented by colored circles, with arrows indicating the happened-before relationship. Data spans, which represent operations on shared state stores, appear as character-labeled squares colored by entity identity. In this specific example, the state stores are databases (Order DB and InsidePayment DB), and their names are displayed above the data spans. The connection between a request and a state access is shown with dashed arrows (solid for writes, hollow for reads). Red highlights and warning symbols mark the potential conflicts identified between the two flows. To focus the visualization on the race condition, we only show the user requests that initiate the flows and the subsequent request spans that access shared state.

The details captured by MICRORACER are critical for analysis. For instance, in request flow B, the Cancel Service invokes the Order Service three times (requests (4), (5), and (7)). MICRORACER distinguishes these requests by their HTTP methods and body content. As shown in Fig. 3, request (4) is the only GET request among them. The other two are PUT requests that perform different update operations: request (5) updates the `status` field of the order entity to 7 (Refunding), whereas request (7) updates it to 4 (Cancelled). Within this single flow, each request is issued only after the previous one has completed, establishing a clear, causally-ordered relationship.

### C. Conflicting Request Pair Identification

After constructing the end-to-end request flows, MICRORACER identifies potential concurrency conflicts by analyzing how different requests interact with shared state resources. The core principle is that two requests are potentially in conflict if they access the same shared data entity, and at least one of them performs a write operation.

1) *Linking Requests to Shared States*: The first step is to precisely identify the shared state accessed by each request. The definition of this state varies across different data stores (e.g., databases, message queues, caches, shared storage) used in microservice systems. We use the link between request spans and their corresponding data spans, which contain the operational details needed to pinpoint the state.

For traditional relational databases, a state corresponds to a specific row within a table. To pinpoint this row, we identify its primary key from the SQL statements captured in the data span. Since detailed schema information is often unavailable, we employ a heuristic approach that matches field names against common primary key indicators like `ID/UID/GUID`, `Key`, or `Serial`. Developers can also provide custom rules to improve the accuracy of this heuristic. For `SELECT`, `UPDATE`, and `DELETE` statements, the `WHERE` clause is parsed to extract the entity-identifying key-value pairs, e.g., `"accountId=4d2a46c7."` For `INSERT` statements, the fields and their corresponding values are extracted directly. Furthermore, to enable a finer-grained analysis that reduces false positives, we also identify the specific columns involved in the operation. Two operations on the same row only conflict if they access an overlapping set of columns.



```

SELECT user_id, document_num, email, gender, password, user_name
FROM user WHERE user_id='4d2a46c7'

UPDATE orders_other SET account_id='4d2a46c7', bought_date=
'2024-05-29' WHERE id='a7e15b90'

INSERT INTO orders_other (account_id, train_number, travel_date, id)
VALUES ('4a2a46c7', 'Z1234', '2024-05-29', 'a7e15b90')

```

Fig. 5. SQL statements executed in TrainTicket during runtime.

Therefore, we parse the SQL to find the columns listed in a SELECT clause, the columns being assigned new values in an UPDATE statement's SET clause, or all columns involved in an INSERT. Fig. 5 illustrates some of the simplified SQL statements executed in the TrainTicket during runtime. The key-value pairs extracted by MICRORACER are highlighted in red. Note that in the UPDATE statement shown in the figure, we extract not only the fields from the WHERE clause (e.g., `account_id`) but also other fields (e.g., `id`). This is because the WHERE clause may use non-primary key conditions to filter the operation targets. Therefore, all ID-related fields in the statement need to be extracted to ensure accurate identification of the database entities affected by the SQL operation.

This principle of identifying a unique state extends to other forms of shared states. For key-value stores like Redis or Memcached, the analysis is more direct, i.e., the entity is the key itself, which we extract from commands like GET, SET, or DEL. For message queues such as Kafka or RabbitMQ, the shared entity is the message stream, identified by the topic or queue name captured from producer or consumer operations. Similarly, for shared object stores like Amazon S3, an entity is a specific object, uniquely identified by its bucket and key, which are recorded from the API call.

After this analysis, each request that interacts with a shared resource is mapped to a precise state, which can be a specific set of database cells, a key-value entry, a message topic, or a storage object. This detailed mapping is the foundation for the subsequent steps of conflict detection.

2) *Identifying Potential Conflicting Request Pairs:* With the specific state for each request identified, MICRORACER systematically filters the vast set of all possible request pairs to find those with a potential for concurrency conflicts. A pair is flagged as a potential conflict only if it satisfies two strict criteria, i.e., the requests must operate on the exact same shared state, and their access patterns must be incompatible (i.e., Read-Write or Write-Write).

The first criterion is to ensure that both requests target the same shared state entity. This requires more than just matching an ID. We enforce two conditions. First, the requests must access the same state store instance, verified using information from the data span like the database IP and name. This check is crucial for preventing false positives where different services might use the same ID value (e.g., an `order_id`) in their own separate, independent databases. Second, the entity identifiers themselves must match (e.g., the same primary key value,

Redis key, or object path). For SQL operations, this means the intersection of their identified primary key sets must be non-empty. To further refine the accuracy for databases, we apply a column-level check. Even if two requests modify the same row, they are not considered conflicting if they operate on mutually exclusive sets of columns. A conflict is only registered if their sets of accessed columns overlap. For example, in Fig. 3, the SQL statements associated with both Request ② and Request ④ contain user ID 4d2a46c7 and order ID a7e15b90, and they access the same column `status`. Therefore, we consider them to be accessing the same shared state entity.

The second criterion is that the request pair must possess a conflicting access pattern. We classify each data store operation as either a Read or a Write. For databases, SELECT is a Read, while INSERT, UPDATE, and DELETE are Writes. For key-value stores, GET is a Read, while SET and DEL are Writes. Any pair consisting of two Read operations is non-conflicting and is discarded. Particularly, this classification is based on the actual operation performed at the data store, not the HTTP method of the incoming service request. Relying on HTTP methods is unreliable; for instance, a service handling an HTTP GET request might internally perform a write operation for logging or caching purposes. In Fig. 3, request ⑥ is an HTTP GET request, but its handling results in an INSERT statement being executed against the database, which is a definitive Write operation. By analyzing the data span, MICRORACER correctly identifies this behavior.

3) *Static Pruning Based on Request Flow:* MICRORACER applies two static pruning strategies to refine the set of conflicting request pairs, thereby significantly narrowing the search space for subsequent validation, i.e., *state store instance pruning* and *flow pruning*.

**State store instance pruning.** This initial filtering step enforces the fundamental rule that a conflict can only occur if two requests access the exact same state store instance. The identity of an instance is determined using connection metadata captured in the data span, such as the database's IP address and name, the key-value store's endpoint, or the message queue's cluster address. MICRORACER is designed to handle complex real-world topologies. For instance, in systems with master-slave database replication or other clustered data stores, a simple endpoint string match might be insufficient. Therefore, we provide a configurable mechanism that allows developers to define rules for what constitutes the "same" logical data store. This ensures, for example, that operations on a primary database and its replica can be correctly identified as interacting with the same shared state.

**Flow pruning.** As we depict in Sec. III-B, after MICRORACER constructs and splits request flows, all known explicit synchronization relationships are taken into account. This includes sequential calls triggered by the same user request, causal synchronization relationships via message queue producer-consumer across different user requests, and mutual exclusion synchronization via distributed locks. Requests within the same request flow have a happened-before relationship, and therefore cannot be sent concurrently. Consequently,

even if they access the same database entity, conflicts will not occur. Based on this feature, we can further eliminate non-concurrent request pairs. Since request spans are linked into request flows through the same flow ID, we only need to check whether the requests in a request pair share the same flow ID.

For asynchronous requests initiated by new threads within the service, we have already handled the divergence and marked them as independent request flows, so they will not be eliminated. For example, in Fig. 4, requests ③ and ④ are marked as belonging to different request flows, so the request pair (3, 4) will still be retained.

#### D. Automated Bug Validation

After identifying suspicious request pairs, MICRORACER begins an automated validation process to confirm which pairs manifest as actual concurrency bugs.

1) *Early Validation for Creation Operations*: The process begins with a fast-pass strategy to identify clear-cut conflicts involving state creation. This check targets pairs where the latter request performs a creation-type operation, such as a database INSERT or a key-value store SET on a new key.

The rationale is that if two requests operate on the same entity identifier and the second one attempts to create it, a conflict is highly probable regardless of the first operation. For example, a SELECT followed by an INSERT on the same entity suggests a query for an object that did not exist moments before its creation, i.e., a logical flaw. Similarly, two consecutive INSERT operations on the same primary key represent a duplicative action that is almost always erroneous, unless the operation is explicitly designed to be idempotent and the system correctly handles the second attempt. This early check efficiently confirms a class of common bugs without requiring full interleaving tests.

2) *Automated Interleaving Testing*: For the remaining suspicious pairs, MICRORACER conducts automated forced interleaving tests to observe if reversing the execution order alters the system’s behavior or final state. The testing process for each request pair ( $\mathcal{A}$ ,  $\mathcal{B}$ ) begins by capturing a snapshot of the relevant state store(s) to serve as a clean baseline. The two requests are then replayed in their original order ( $\mathcal{A} \rightarrow \mathcal{B}$ ), and all relevant outputs (e.g., service logs, request responses, and the final state of the affected stores) are collected. Following this forward execution, the state is reverted to the initial snapshot. Next, the requests are replayed in the reverse order ( $\mathcal{B} \rightarrow \mathcal{A}$ ), and the same set of data is collected again. Upon completion, the state is restored one final time, ensuring a clean environment for testing the next suspicious pair.

3) *The Testing Oracle*: Upon gathering the information from each suspicious request pair through interleaving testing, we submit each pair’s data to the oracle. The oracle then executes a three-stage validation process to ascertain whether each pair triggers a concurrency bug. This validation process is grounded on the principle of comparing the behavior of request pairs under different execution orders, excluding variables like timestamps, system metrics, or other environment-specific details that do not reflect the impact of order changes.

- *Service-level Validation*: We compare the logs of the involved services under the two interleaving orders of execution. If there is a discrepancy between the two orders, such as a service throwing an exception in one order but not in the other, we can deduce that this request pair triggers a concurrency bug.
- *Response-level Validation*: We compare the corresponding responses of the same request across the two orders. If the responses differ, it is evident that the request’s outcome is influenced by the execution order, indicating that the pair meets the criteria for concurrency bugs.
- *State-level Validation*: We compare the final state snapshots of the involved data stores. Any divergence in the final stored data between the two runs indicates a data inconsistency bug. To reduce false positives in systems with weak consistency models (e.g., a social platform where eventual consistency is acceptable), we provide an optional interface. It allows developers to specify invariants or expected final values for specific data fields, enabling MICRORACER to distinguish between benign, business-allowed inconsistencies and true data corruption bugs.

Through these three stages, conflicting request pairs can be effectively identified. Moreover, the stages are designed to progressively unveil the effects of concurrency bugs from a multi-level perspective. This methodology helps developers understand the impact of concurrency issues, thereby facilitating the remediation of bugs.

## IV. IMPLEMENTATION

We implement MICRORACER in Python. For instrumentation and request flow construction, MICRORACER leverages the telemetry capabilities of Apache SkyWalking [33], a distributed tracing system for cloud service system architectures. Its multi-language instrumentation support (e.g., Java/Python/Go) and extensive library coverage enable MICRORACER’s multi-language service testing capability. Take Java-based services as an example, MICRORACER collects request spans by instrumenting HTTP libraries (Spring-MVC/RestTemplate) and data spans through JDBC instrumentation. MICRORACER can also incorporate trace data collected from middleware components such as cache and message queues into the request flow construction and analysis. It then automatically extracts request flows from the aggregated trace data, and performs concurrent bug detection.

To support automated interleaving testing, we enhance SkyWalking plugins to log the complete request and response payloads in traces. This includes the full headers and body for HTTP and the method, parameters, and return values for various RPC protocols. This allows MICRORACER to precisely replay request contexts during analysis. Particularly, while implemented with SkyWalking, MICRORACER can analyze telemetry data generated by other frameworks (such as OpenTelemetry) with minimal adaptation to the data format.

## V. EXPERIMENTAL EVALUATION

In this section, we evaluate the performance of MICRO-RACER for concurrency bug detection. Particularly, we aim to answer the following two research questions:

- **RQ1:** Can MICRO-RACER identify potential conflict request pairs?
- **RQ2:** Can MICRO-RACER detect concurrency bugs in microservice systems?

### A. Experiment Setting

1) *Microservice Benchmarks:* We select four popular open-source microservice systems for our experiments, including TrainTicket [16], Bank of Anthos [17], and two microservice applications from DeathStarBench (i.e., Social Network and Media Service) [18]. Among them, both the TrainTicket and DeathStarBench have been confirmed to have concurrency issues in previous studies [5], [16] (the bugs in TrainTicket are reproduced from industrial failures). In addition to the known concurrency bugs, we also inject bugs from previous studies [11] for a more comprehensive evaluation.

- **TrainTicket:** TrainTicket [16] is a railway ticketing application based on microservice architecture, which has been widely used in many microservice-related studies [34], [35]. It consists of 41 services implemented in different programming languages such as Java, Go, Node.js, Python, providing users with functionalities such as ticket query, booking, and payment. Most business functionalities in TrainTicket are implemented using cross-service calls, requiring the collaboration of multiple microservices. The most complex business logic is the ticket booking function, whose call graph involves over ten services.
- **Bank of Anthos:** Bank of Anthos [17] is a microservice app open-sourced by Google, consisting of five services developed in Java and Python. It simulates core banking operations including account management and payment processing. The benchmark demonstrates typical financial transaction workflows through inter-service communication, with the payment function representing its most complex business logic involving multiple service interactions.
- **DeathStarBench:** DeathStarBench [18] is a popular benchmark suite for microservices, which includes four cloud applications, primarily developed in C++. Our experiments are conducted on the Social Network and Media Service. Social Network is a social application comprising 12 services, using Thrift RPCs to coordinate various services to implement functionalities such as post creation, browsing, and searching. Media Service is a review application consisting of 13 services. It provides external HTTP endpoints for functionalities such as user registration, review writing, and movie information publishing.

2) *Concurrency Bug Replication:* For TrainTicket [36], we minimize source code modifications based on the original business processes to reproduce the concurrency bugs. For bugs that require specific architectures (e.g., master-slave databases), we also make minimal deployment configuration

changes to meet the reproduction requirements. To collect distributed tracing data, we deploy SkyWalking agents in each service. For the experimental workload scripts, we use the automated request scripts provided by TrainTicket and ensure the workload triggers the concurrency fault-related code.

For the other three benchmarks, we deploy and modify the source code along with database configurations to reproduce the faults. We employ the built-in functional test scripts as workloads since they already provide comprehensive coverage of executable user requests. Similar to TrainTicket, we deploy SkyWalking agents across all services of Bank of Anthos to collect trace data. For the DeathStarBench, since the Social Network and Media services (C++-based systems) are not supported by SkyWalking, we directly utilize their built-in Jaeger trace information for request flow analysis.

### B. Experimental Results

1) *The Effectiveness of Conflict Request Pair Identification (RQ1):* To answer RQ1, we evaluate how effectively MICRO-RACER prunes the search space for potential conflicts. We establish a baseline using Random Testing, which represents a naive approach where a developer considers all possible request pairs that have at least one write conflict on the same state entity. The total number of such pairs for each case is shown as “Random Pairs” in Table I. Our results demonstrate that MICRO-RACER’s two-stage pruning strategy is highly effective. Fig. 6 visually confirms this, showing a stacked bar chart for all 14 test cases. The overwhelming proportion of “Pruned” sections (light gray) in most cases illustrates the strategy’s ability in narrowing the search space.

Quantitatively, our method reduces the number of candidate pairs requiring validation by an average of 79% compared to the random baseline. This is achieved through two sequential pruning stages detailed in Table I. The first stage of pruning leverages state instance information. By enforcing that conflicting requests must target the same state instance, not just a similarly named entity, MICRO-RACER filters out a significant number of false candidates. As shown by the “Instance Pruning” column in Table I, this step alone eliminates an average of 73% of the pairs from the random baseline. The second stage applies the request flow analysis. Using the happened-before relationships established during flow construction, MICRO-RACER discards pairs that have a sequential relationship within the same flow and thus cannot be concurrent. The “Flow Pruning” column in Table I shows this step further removes an additional 6% of non-concurrent pairs on average.

The small set of pairs remaining after these stages (the green “True Positive” and pink “False Positive” bars in Fig. 6) are the high-potential candidates passed to the validation phase. It is worth noting that in Case 4 (TrainTicket), the initial number of “Random Pairs” is unusually low (only 9). This is because the specific fault in this case triggers a fatal error, causing the workload to terminate prematurely. The resulting truncated trace contains very few database write operations, naturally limiting the number of potential conflicts.



TABLE I

EXPERIMENTS RESULT. “EARLY VALIDATION” SHOWS THE NUMBER OF REQUEST PAIRS THAT CAN BE CONFIRMED AS CONFLICTS EARLY, ALL CONSIDERED AS POSITIVES. “AUTO TEST” SHOWS THE NUMBER OF REQUEST PAIRS THAT NEED TO BE VERIFIED THROUGH AUTOMATED INTERLEAVING TESTING. “FP” AND “TP” DISPLAY THE NUMBERS OF FALSE POSITIVES AND TRUE POSITIVES, RESPECTIVELY. FOR TRUE POSITIVES, THE “(X+Y)” INDICATE THAT X PAIRS ARE IDENTIFIED THROUGH EARLY VALIDATION, WHILE Y PAIRS THROUGH AUTOMATED INTERLEAVING TESTING.

Case	Benchmark	Request Spans	Data Spans	Request Flows	Random Pairs	Instance Pruning	Flow Pruning	Early Validation	Auto Test	FP	TP
1	TrainTicket	63	81	10	78	-56	-5	6	11	2	11 (6+5)
2	TrainTicket	56	78	11	76	-61	-3	5	7	0	9 (5+4)
3	TrainTicket	55	75	11	68	-50	-3	6	9	5	9 (6+3)
4	TrainTicket	69	84	11	9	-7	-1	1	0	0	1 (1+0)
5	TrainTicket	59	83	13	99	-80	-3	9	7	6	10 (9+1)
6	Bank of Anthos	10	16	8	28	-12	-5	5	6	0	7 (5+2)
7	Bank of Anthos	10	16	8	28	-12	-3	7	6	0	9 (7+2)
8	Bank of Anthos	14	17	9	49	-41	-1	3	4	3	4 (3+1)
9	Bank of Anthos	15	19	8	36	-28	-4	4	0	0	4 (4+0)
10	SocialNetwork	23	32	9	91	-72	-3	8	8	3	11 (8+3)
11	SocialNetwork	24	34	10	98	-76	-3	9	10	1	15 (9+6)
12	MediaService	20	29	3	64	-53	-2	4	5	0	6 (4+2)
13	MediaService	26	41	5	75	-64	-2	6	3	2	7 (6+1)
14	MediaService	21	32	5	62	-51	-1	6	4	2	7 (6+1)

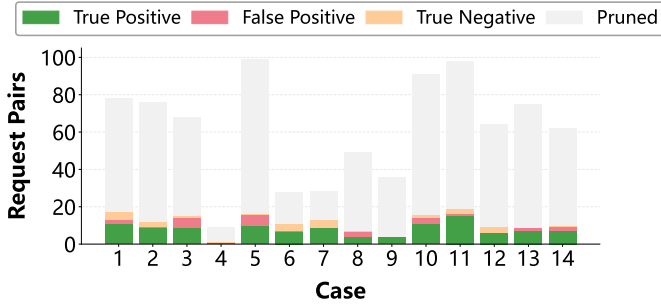


Fig. 6. The effectiveness of the pruning strategy. The “Pruned” section represents pairs excluded by MICRORACER.

In summary, by systematically applying constraints based on both state locality and causal dependencies, MICRORACER dramatically reduces the search space, making automated validation computationally feasible. Moreover, since it operates at the system level, a single analysis can generate candidate pairs covering multiple distinct concurrency faults, provided the workload has sufficient service coverage.

2) *The Effectiveness of Concurrency Bug Detection (RQ2)*: Our experiments show that MICRORACER is effective at detecting concurrency bugs. As shown in the “TP” (True Positives) column of Table I, MICRORACER successfully identifies all replicated concurrency faults across four benchmarks, with six detected through early validation and five through automated interleaving testing. Particularly, MICRORACER detects a previously unknown bug in the Bank of Anthos benchmark, which is not introduced through our fault injection. We will discuss it in our first case study (Sec. V-C).

While effective, the framework does produce a small number of false positives (FPs). Our analysis reveals that the primary source of these FPs is a specific and identifiable pattern: benign race conditions involving pure query requests. These are read-only requests intended to retrieve data for

frontend displays or to monitor system status, where variations in response data are expected and do not indicate a data corruption bug. The mechanism causing these FPs lies within our response-level validation oracle. When a pure query request races with a write operation, its response content will naturally differ depending on whether it executes before or after the write. For example:

- In Case 1, the FPs include a request to `GET /securityservice/securityConfigs/{accountId}`. This endpoint queries recent user activity to detect abnormal behavior. While its purpose is for security, its operation is a simple database read. Racing with a write causes its response to change, triggering an FP.
- In Case 5, the six FPs all involve the request of `GET /orderOtherService/orderOther/refresh`, which fetches all of a user’s order data. When this races with a request that modifies an order, the list of returned orders changes, which our oracle flags as an inconsistency.

This behavior is a known limitation of automated validation that relies on stateless response comparison. To address this and empower developers to refine the analysis, MICRORACER includes a practical whitelist mechanism. Testers can use this feature to provide domain-specific knowledge by marking specific read-only endpoints where response variations are benign and expected. By exempting these configured interfaces from response-level validation, the number of false positives can be significantly reduced with minimal manual effort.

### C. Case Studies

To illustrate the practical application and effectiveness of MICRORACER, we present three concrete case studies.

- **Case 1:** This case study highlights a classic check-then-act race condition within the Bank of Anthos benchmark. The vulnerability arises when two valid, independent transfer requests are processed concurrently by the LedgerWriter service. The service’s logic first performs a balance check

(the “check”) and then executes the transfer (the “act”). However, without proper locking or atomic operations, a critical window exists between these two steps. This allows both requests to read the initial balance and pass the funds validation before either can update the account. Consequently, both transfers are committed, leading to an unauthorized overdraft. This bug bypasses the existing idempotency logic, which is not designed to enforce atomicity for concurrent, non-duplicate operations.

- **Case 2:** This case demonstrates the detection of the classic inter-service race condition between payment and cancellation flows, as detailed in Sec. II-C. MICRORACER identifies the conflicting request pairs (highlighted in Fig. 3) and subjects them to automated interleaving tests. The tests reveal a critical behavioral inconsistency: the service’s HTTP response for the cancellation operation differs depending on the execution order. This allows the response-level validation mechanism to confirm the bug, correctly reporting both pairs as true positives.
- **Case 3:** This case demonstrates a classic read-modify-write atomicity violation. In the replicated TrainTicket scenario, two requests initiated via the Preserve Service attempt to reserve the last available seat from the Seat Service concurrently. A race condition occurs when the first request reads the seat availability (count = 1) but is delayed before it can write the update (decrementing the count to 0). During this critical window, the second request also reads the seat count as 1 and proceeds. Consequently, both purchase requests succeed, causing the seat to be oversold and violating data integrity.

## VI. THREATS TO VALIDITY

**External Validity.** The generalizability of our findings is constrained by our evaluation’s reliance on a specific set of open-source microservice benchmarks. These systems may not capture the full diversity of architectures, workloads, or data store technologies used in all industrial applications. To mitigate this, we select benchmarks that are complex, widely used in both academic and industrial research, and considered representative of common microservice patterns. Furthermore, the bugs we reproduce reflect prevalent and challenging concurrency issues, suggesting that MICRORACER’s effectiveness is likely applicable to a broader range of real-world systems.

**Construct Validity.** The primary threat to construct validity concerns the accuracy with which MICRORACER identifies shared entities and confirms bugs.

First, identifying the specific entity being accessed relies on a heuristic to parse primary key values from SQL statements. This approach can be imprecise for highly complex queries or those that filter on non-primary-key attributes (e.g., `SELECT * FROM orders WHERE order_time < '2024-06-01';`). This may cause MICRORACER to miss certain conflicts, leading to potential false negatives. We acknowledge this as a fundamental challenge of SQL analysis. Therefore, our design allows developers to refine heuristics when ambiguities arise.

Second, MICRORACER’s black-box nature presents a risk of false positives. It detects data races at the data store level but cannot inspect an application’s internal source code. A service might implement its own synchronization logic (e.g., optimistic locking using version numbers or Compare-and-Swap operations) that correctly handles a data race. Because this code-level logic is invisible to our instrumentation, MICRORACER may flag such a benign race as a bug. While our multi-level validation oracle helps filter many cases, this remains a limitation inherent to any black-box testing approach.

## VII. RELATED WORK

**Static Analysis.** Static analysis emerges as a proactive technique for identifying potential concurrency issues without the necessity of code execution. For example, to identify deadlocks that may arise from the integration of test control mechanisms, Chen et al. [37] proposed an approach that leverages static analysis to construct test constraints, with a particular focus on synchronization events. Lu et al. [38] introduced a tool that combines static analysis, log mining [39], and log enhancement techniques to efficiently detect concurrency bugs in distributed systems. By converting concurrency bug detection into a source-sink reachability problem, Cai et al. [40] presented a value-flow analysis framework for statically finding diversified inter-thread value-flow bugs. These methods play a crucial role in the early detection of problems during the development phase, thus preemptively addressing issues that could lead to runtime errors. However, static methods do not always excel at detecting concurrent bugs, given the inherent complexity of the runtime environment in distributed systems.

**Dynamic Analysis.** Dynamic analysis plays a pivotal role in the detection of concurrency issues by executing the system and monitoring its runtime behaviors. It provides a real-time perspective on how concurrent operations interact within a system. For example, built with a set of happens-before rules that model various communication and concurrency mechanisms, DCatch [12] predicts distributed concurrency bugs by analyzing correct execution of distributed systems. Similar to our work, ReqRacer [11] employs the construction of a dependency graph to identify potential conflict-prone request pairs for interleaving testing. Yuan et al. [41] used partial order sampling and conflict analysis to efficiently test Erlang-based systems. Focusing on scalability, FlyMC [42] presents a tool for scalable testing of complex interleavings in distributed systems to detect concurrency bugs. Meanwhile, Wu et al. [43] targeted efficiency by identifying repeated interleavings, which is a pattern often found in concurrency bug detectors. However, these approaches are tailored for traditional distributed systems and do not address the challenges unique to microservice architecture, which often employs a “database-per-service” design pattern.

**Machine Learning and AI.** Recent advancements in AI and machine learning have been applied to concurrency testing to improve the efficiency and effectiveness of detecting issues. Zhang et al. [44] presented a system that uses AI to tolerate concurrency bugs, which can be particularly useful

in distributed environments where bugs are hard to eradicate. Mukherjee et al. [45] introduced a framework called QL that uses reinforcement learning to explore the space of possible interleavings in concurrent programs, adapting to the program under test. While seemingly general and powerful, Machine Learning and AI techniques often demand substantial computational resources for training. Additionally, they introduce a level of uncertainty due to their nature as black box models.

## VIII. CONCLUSION

In this work, we introduce MICRORACER, an non-intrusive and automated framework for detecting concurrency bugs in microservice systems. MICRORACER first leverages dynamic instrumentation of widely-used libraries, effectively capturing detailed trace data without modifications to the application code. These data enable the analysis of happened-before relationships and resource access patterns among common operations in service systems. MICRORACER then identifies suspicious request pairs to check the correctness of their concurrency behaviors. In this process, MICRORACER applies static pruning strategies to improve the search efficiency. Finally, MICRORACER validates the concurrency bugs through a three-stage process. Overall, MICRORACER can effectively address the challenges of complex dependencies and the need for accurate, automated bug validation. Experiments on four widely-used open-source microservice benchmarks with replicated industrial bugs demonstrate MICRORACER's ability to accurately and efficiently detect concurrency bugs.

## ACKNOWLEDGEMENT

This work is supported by the National Natural Science Foundation of China (No. 62402536).

## REFERENCES

- [1] S. He, B. Feng, L. Li, X. Zhang, Y. Kang, Q. Lin, S. Rajmohan, and 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, ESEC/FSE 2023, San Francisco, CA, USA, December 3-9, 2023*. ACM, 2023, pp. 1750–1761. [Online]. Available: <https://doi.org/10.1145/3611643.3613881>
- [2] H. Zhou, M. Chen, Q. Lin, Y. Wang, X. She, S. Liu, R. Gu, B. C. Ooi, and J. Yang, "Overload control for scaling wechat microservices," in *Proceedings of the ACM Symposium on Cloud Computing, SoCC 2018, Carlsbad, CA, USA, October 11-13, 2018*. ACM, 2018, pp. 149–161. [Online]. Available: <https://doi.org/10.1145/3267809.3267823>
- [3] Z. Chen, Y. Kang, L. Li, X. Zhang, H. Zhang, H. Xu, Y. Zhou, L. Yang, J. Sun, Z. Xu, Y. Dang, F. Gao, P. Zhao, B. Qiao, Q. Lin, D. Zhang, and M. R. Lyu, "Towards intelligent incident management: why we need it and how we make it," in *ESEC/FSE '20: 28th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, Virtual Event, USA, November 8-13, 2020*. ACM, 2020, pp. 1487–1497. [Online]. Available: <https://doi.org/10.1145/3368089.3417055>
- [4] L. Tang, C. Bhandari, Y. Zhang, A. Karanika, S. Ji, I. Gupta, and T. Xu, "Fail through the cracks: Cross-system interaction failures in modern cloud systems," in *Proceedings of the Eighteenth European Conference on Computer Systems, EuroSys 2023, Rome, Italy, May 8-12, 2023*. ACM, 2023, pp. 433–451. [Online]. Available: <https://doi.org/10.1145/3552326.3587448>
- [5] J. F. Loff, D. Porto, J. Garcia, J. Mace, and R. Rodrigues, "Antipode: Enforcing cross-service causal consistency in distributed applications," in *Proceedings of the 29th Symposium on Operating Systems Principles, SOSP 2023, Koblenz, Germany, October 23-26, 2023*. ACM, 2023, pp. 298–313. [Online]. Available: <https://doi.org/10.1145/3600006.3613176>
- [6] T. Leesatapornwongsa, J. F. Lukman, S. Lu, and H. S. Gunawi, "Taxdc: A taxonomy of non-deterministic concurrency bugs in datacenter distributed systems," in *Proceedings of the Twenty-First International Conference on Architectural Support for Programming Languages and Operating Systems, ASPLOS 2016, Atlanta, GA, USA, April 2-6, 2016*. ACM, 2016, pp. 517–530. [Online]. Available: <https://doi.org/10.1145/2872362.2872374>
- [7] J. Li, Y. Zhang, S. Lu, H. S. Gunawi, X. Gu, F. Huang, and D. Li, "Performance bug analysis and detection for distributed storage and computing systems," *ACM Trans. Storage*, vol. 19, no. 3, pp. 23:1–23:33, 2023. [Online]. Available: <https://doi.org/10.1145/3580281>
- [8] J. Li, Y. Chen, H. Liu, S. Lu, Y. Zhang, H. S. Gunawi, X. Gu, X. Lu, and D. Li, "Pcatch: automatically detecting performance cascading bugs in cloud systems," in *Proceedings of the Thirteenth EuroSys Conference, EuroSys 2018, Porto, Portugal, April 23-26, 2018*. ACM, 2018, pp. 7:1–7:14. [Online]. Available: <https://doi.org/10.1145/3190508.3190552>
- [9] H. Liu, X. Wang, G. Li, S. Lu, F. Ye, and C. Tian, "Fetch: Automatically detecting time-of-fault bugs in cloud systems," in *Proceedings of the Twenty-Third International Conference on Architectural Support for Programming Languages and Operating Systems, ASPLOS 2018, Williamsburg, VA, USA, March 24-28, 2018*. ACM, 2018, pp. 419–431. [Online]. Available: <https://doi.org/10.1145/3173162.3177161>
- [10] S. Koch, T. Sauer, M. Johns, and G. Pellegrino, "Raccoon: automated verification of guarded race conditions in web applications," in *SAC '20: The 35th ACM/SIGAPP Symposium on Applied Computing, online event, [Brno, Czech Republic], March 30 - April 3, 2020*. ACM, 2020, pp. 1678–1687. [Online]. Available: <https://doi.org/10.1145/3341105.3373855>
- [11] Z. Qiu, S. Shao, Q. Zhao, and G. Jin, "Understanding and detecting server-side request races in web applications," in *ESEC/FSE '21: 29th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, Athens, Greece, August 23-28, 2021*. ACM, 2021, pp. 842–854. [Online]. Available: <https://doi.org/10.1145/3468264.3468594>
- [12] H. Liu, G. Li, J. F. Lukman, J. Li, S. Lu, H. S. Gunawi, and C. Tian, "Dcatch: Automatically detecting distributed concurrency bugs in cloud systems," in *Proceedings of the Twenty-Second International Conference on Architectural Support for Programming Languages and Operating Systems, ASPLOS 2017, Xi'an, China, April 8-12, 2017*. ACM, 2017, pp. 677–691. [Online]. Available: <https://doi.org/10.1145/3037697.3037735>
- [13] V. Heorhiadi, S. Rajagopalan, H. Jamjoom, M. K. Reiter, and V. Sekar, "Gremlin: Systematic resilience testing of microservices," in *36th IEEE International Conference on Distributed Computing Systems, ICDCS 2016, Nara, Japan, June 27-30, 2016*. IEEE Computer Society, 2016, pp. 57–66. [Online]. Available: <https://doi.org/10.1109/ICDCS.2016.11>
- [14] C. S. Meiklejohn, A. Estrada, Y. Song, H. Miller, and R. Padhye, "Service-level fault injection testing," in *SoCC '21: ACM Symposium on Cloud Computing, Seattle, WA, USA, November 1 - 4, 2021*. ACM, 2021, pp. 388–402. [Online]. Available: <https://doi.org/10.1145/3472883.3487005>
- [15] Z. Long, G. Wu, X. Chen, C. Cui, W. Chen, and J. Wei, "Fitness-guided resilience testing of microservice-based applications," in *2020 IEEE International Conference on Web Services, ICWS 2020, Beijing, China, October 19-23, 2020*. IEEE, 2020, pp. 151–158. [Online]. Available: <https://doi.org/10.1109/ICWS49710.2020.00027>
- [16] X. Zhou, X. Peng, T. Xie, J. Sun, C. Ji, W. Li, and D. Ding, "Fault analysis and debugging of microservice systems: Industrial survey, benchmark system, and empirical study," *IEEE Trans. Software Eng.*, vol. 47, no. 2, pp. 243–260, 2021. [Online]. Available: <https://doi.org/10.1109/TSE.2018.2887384>
- [17] "Bank of anthos," <https://github.com/GoogleCloudPlatform/bank-of-anthos>, 2019, accessed: 2025-07-20.
- [18] Y. Gan, Y. Zhang, D. Cheng, A. Shetty, P. Rath, N. Katarki, A. Bruno, J. Hu, B. Ritchken, B. Jackson, K. Hu, M. Pancholi, Y. He, B. Clancy, C. Colen, F. Wen, C. Leung, S. Wang, L. Zaruvinsky, M. Espinosa, R. Lin, Z. Liu, J. Padilla, and C. Delimitrou, "An open-source benchmark suite for microservices and their hardware-software implications for cloud & edge systems," in *Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems, ASPLOS 2019, Providence, RI, USA, April 13-17, 2019*. ACM, 2019, pp. 3–18. [Online]. Available: <https://doi.org/10.1145/3297858.3304013>

- [19] R. Fonseca, G. Porter, R. H. Katz, S. Shenker, and I. Stoica, "X-trace: A pervasive network tracing framework," in *4th Symposium on Networked Systems Design and Implementation (NSDI 2007)*, April 11-13, 2007, Cambridge, Massachusetts, USA, *Proceedings*. USENIX, 2007. [Online]. Available: <http://www.usenix.org/events/nsdi07/tech/fonseca.html>
- [20] B. H. Sigelman, L. A. Barroso, M. Burrows, P. Stephenson, M. Plakal, D. Beaver, S. Jaspán, and C. Shanbhag, "Dapper, a large-scale distributed systems tracing infrastructure," 2010.
- [21] J. Mace, R. Roelke, and R. Fonseca, "Pivot tracing: dynamic causal monitoring for distributed systems," in *Proceedings of the 25th Symposium on Operating Systems Principles, SOSP 2015*, Monterey, CA, USA, October 4-7, 2015. ACM, 2015, pp. 378–393. [Online]. Available: <https://doi.org/10.1145/2815400.2815415>
- [22] J. Kaldor, J. Mace, M. Bejda, E. Gao, W. Kuropatwa, J. O'Neill, K. H. Ong, B. Schaller, P. Shan, B. Viscomi, V. Venkataraman, K. Veeraraghavan, and Y. J. Song, "Canopy: An end-to-end performance tracing and analysis system," in *Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai, China, October 28-31, 2017*. ACM, 2017, pp. 34–50. [Online]. Available: <https://doi.org/10.1145/3132747.3132749>
- [23] 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, and R. Nie, "Network-centric distributed tracing with deepflow: Troubleshooting your microservices in zero code," in *Proceedings of the ACM SIGCOMM 2023 Conference, ACM SIGCOMM 2023, New York, NY, USA, 10-14 September 2023*. ACM, 2023, pp. 420–437. [Online]. Available: <https://doi.org/10.1145/3603269.3604823>
- [24] Z. Chen, J. Pu, and Z. Zheng, "Tracezip: Efficient distributed tracing via trace compression," *Proc. ACM Softw. Eng.*, vol. 2, no. ISSTA, Jun. 2025. [Online]. Available: <https://doi.org/10.1145/3728888>
- [25] L. Zhang, Z. Xie, V. Anand, Y. Vigfusson, and J. Mace, "The benefit of hindsight: Tracing edge-cases in distributed systems," in *20th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2023, Boston, MA, April 17-19, 2023*. USENIX Association, 2023, pp. 321–339. [Online]. Available: <https://www.usenix.org/conference/nsdi23/presentation/zhang-lei>
- [26] Y. Wu, A. Chen, and L. T. X. Phan, "Zeno: Diagnosing performance problems with temporal provenance," in *16th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2019, Boston, MA, February 26-28, 2019*. USENIX Association, 2019, pp. 395–420. [Online]. Available: <https://www.usenix.org/conference/nsdi19/presentation/wu>
- [27] S. Luo, H. Xu, C. Lu, K. Ye, G. Xu, L. Zhang, Y. Ding, J. He, and C. Xu, "Characterizing microservice dependency and performance: Alibaba trace analysis," in *SoCC '21: ACM Symposium on Cloud Computing, Seattle, WA, USA, November 1 - 4, 2021*. ACM, 2021, pp. 412–426. [Online]. Available: <https://doi.org/10.1145/3472883.3487003>
- [28] Z. Zhang, M. K. Ramanathan, P. Raj, A. Parwal, T. Sherwood, and M. Chabbi, "CRISP: critical path analysis of large-scale microservice architectures," in *2022 USENIX Annual Technical Conference, USENIX ATC 2022, Carlsbad, CA, USA, July 11-13, 2022*. USENIX Association, 2022, pp. 655–672. [Online]. Available: <https://www.usenix.org/conference/atc22/presentation/zhang-zhizhou>
- [29] "Trainticket fault replicate," <https://github.com/FudanSELab/train-ticket-fault-replicate/tree/ts-error-F13-zipkin>, 2018, accessed: 2024-04-22.
- [30] X. Li, Y. Chen, and Z. Lin, "Towards automated inter-service authorization for microservice applications," in *Proceedings of the ACM SIGCOMM 2019 Conference Posters and Demos, SIGCOMM 2019, Beijing, China, August 19-23, 2019*. ACM, 2019, pp. 3–5. [Online]. Available: <https://doi.org/10.1145/3342280.3342288>
- [31] T. Cerný, A. S. Abdelfattah, V. Bushong, A. A. Maruf, and D. Taibi, "Microvision: Static analysis-based approach to visualizing microservices in augmented reality," in *IEEE International Conference on Service-Oriented System Engineering, SOSE 2022, Newark, CA, USA, August 15-18, 2022*. IEEE, 2022, pp. 49–58. [Online]. Available: <https://doi.org/10.1109/SOSE55356.2022.00012>
- [32] V. Bushong, D. Das, and T. Cerný, "Reconstructing the holistic architecture of microservice systems using static analysis," in *Proceedings of the 12th International Conference on Cloud Computing and Services Science, CLOSER 2022, Online Streaming, April 27-29, 2022*. SCITEPRESS, 2022, pp. 149–157. [Online]. Available: <https://doi.org/10.5220/0011032100003200>
- [33] "Apache skywalking," <https://skywalking.apache.org/>, 2017, accessed: 2024-06-05.
- [34] X. Peng, C. Zhang, Z. Zhao, A. Isami, X. Guo, and Y. Cui, "Trace analysis based microservice architecture measurement," in *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, ESEC/FSE 2022, Singapore, Singapore, November 14-18, 2022*. ACM, 2022, pp. 1589–1599. [Online]. Available: <https://doi.org/10.1145/3540250.3558951>
- [35] Z. Chen, Z. Jiang, Y. Su, M. R. Lyu, and Z. Zheng, "Tracemesh: Scalable and streaming sampling for distributed traces," in *17th IEEE International Conference on Cloud Computing, CLOUD 2024, Shenzhen, China, July 7-13, 2024*, R. N. Chang, C. K. Chang, J. Yang, N. L. Atukorala, Z. Jin, M. Sheng, J. Fan, K. Fletcher, Q. He, T. Kosar, S. Sarkar, S. Venkateswaran, S. Wang, X. Liu, S. Seelam, C. Narayanaswami, and Z. Zong, Eds. IEEE, 2024, pp. 54–65. [Online]. Available: <https://doi.org/10.1109/CLOUD62652.2024.00016>
- [36] "Trainticket:v1.0," <https://github.com/FudanSELab/train-ticket>, 2022, accessed: 2025-07-20.
- [37] J. Chen, "On using static analysis in distributed system testing," in *Engineering Distributed Objects, Second International Workshop, EDO 2000, Davis, CA, USA, November 2-3, 2000, Revised Papers*, ser. Lecture Notes in Computer Science, vol. 1999. Springer, 2000, pp. 145–162. [Online]. Available: [https://doi.org/10.1007/3-540-45254-0\\_13](https://doi.org/10.1007/3-540-45254-0_13)
- [38] J. Lu, F. Li, C. Liu, L. Li, X. Feng, and J. Xue, "Clouddroid: Detecting distributed concurrency bugs via log mining and enhancement," *IEEE Trans. Software Eng.*, vol. 48, no. 2, pp. 662–677, 2022. [Online]. Available: <https://doi.org/10.1109/TSE.2020.2999364>
- [39] S. He, P. He, Z. Chen, T. Yang, Y. Su, and M. R. Lyu, "A survey on automated log analysis for reliability engineering," *ACM Comput. Surv.*, vol. 54, no. 6, pp. 130:1–130:37, 2022. [Online]. Available: <https://doi.org/10.1145/3460345>
- [40] Y. Cai, P. Yao, and C. Zhang, "Canary: practical static detection of inter-thread value-flow bugs," in *PLDI '21: 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation, Virtual Event, Canada, June 20-25, 2021*. ACM, 2021, pp. 1126–1140. [Online]. Available: <https://doi.org/10.1145/3453483.3454099>
- [41] X. Yuan and J. Yang, "Effective concurrency testing for distributed systems," in *ASPLOS '20: Architectural Support for Programming Languages and Operating Systems, Lausanne, Switzerland, March 16-20, 2020*. ACM, 2020, pp. 1141–1156. [Online]. Available: <https://doi.org/10.1145/3373376.3378484>
- [42] J. F. Lukman, H. Ke, C. A. Stuardo, R. O. Suminto, D. H. Kurniawan, D. Simon, S. Priambada, C. Tian, F. Ye, T. Leesatapornwongsa, A. Gupta, S. Lu, and H. S. Gunawi, "Flymc: Highly scalable testing of complex interleavings in distributed systems," in *Proceedings of the Fourteenth EuroSys Conference 2019, Dresden, Germany, March 25-28, 2019*. ACM, 2019, pp. 20:1–20:16. [Online]. Available: <https://doi.org/10.1145/3302424.3303986>
- [43] Z. Wu, K. Lu, and X. Wang, "Identifying repeated interleavings to improve the efficiency of concurrency bug detection," in *Algorithms and Architectures for Parallel Processing - 15th International Conference, ICA3PP 2015, Zhangjiajie, China, November 18-20, 2015. Proceedings, Part IV*, ser. Lecture Notes in Computer Science, vol. 9531. Springer, 2015, pp. 175–188. [Online]. Available: [https://doi.org/10.1007/978-3-319-27140-8\\_13](https://doi.org/10.1007/978-3-319-27140-8_13)
- [44] M. Zhang, Y. Wu, S. Lu, S. Qi, J. Ren, and W. Zheng, "AI: a lightweight system for tolerating concurrency bugs," in *Proceedings of the 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering, (FSE-22), Hong Kong, China, November 16 - 22, 2014*. ACM, 2014, pp. 330–340. [Online]. Available: <https://doi.org/10.1145/2635868.2635885>
- [45] S. Mukherjee, P. Deligiannis, A. Biswas, and A. Lal, "Learning-based controlled concurrency testing," *Proc. ACM Program. Lang.*, vol. 4, no. OOPSLA, pp. 230:1–230:31, 2020. [Online]. Available: <https://doi.org/10.1145/3428298>