The next AMPLab: Real-time Intelligent Secure Execution

Ion Stoica

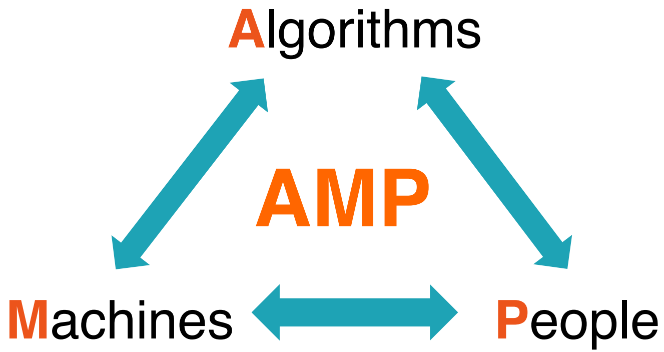
October 26, 2016

databricks

Berkeley's AMPLab

2011 – 2016

- Mission: "*Make sense of big data*"
- 8 faculty, 60+ students



Governmental and industrial founding

AMPLab Goal and Impact

Goal: Next generation of open source data analytics stack for industry & academia

Berkeley Data Analytics Stack (BDAS)

APACHE Spark™ Apache MESOS™ ALLUXIO ...

What is next?

RISE: Real-time Intelligent Secure Execution

databricks

RISELab

From live data to real-time decisions

AMPLab

From batch data to advanced analytics

Why?

Data only as valuable as the decisions it enables

Harvard Business Review

MANAGING ORGANIZATIONS

How the Big Data Explosion Has Changed Decision Making

by Michael Schrage

AUGUST 25, 2016

SAVE | SHARE | COMMENT | TEXT SIZE | PRINT | $8.95 BUY COPIES

DataInformed
Big Data and Analytics in the Enterprise

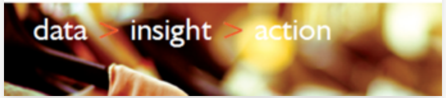
Advanced Analytics | Cloud | Customer Analytics

eBooks | Events | Glossary | University Map | Use Cases

How to Turn Big Data into Insights and Action

by Bernard Marr | May 18, 2016 5:30 am | 1 Comments

actionableinsight



BIG DATA

3 Ways Big Data Analytics Is Changing The Way Decisions Are Made

Forrester's 2016 Predictions: Turn Data Into Insight And Action

Posted by Brian Hopkins on November 9, 2015

Why?

Data only as valuable as the decisions it enables

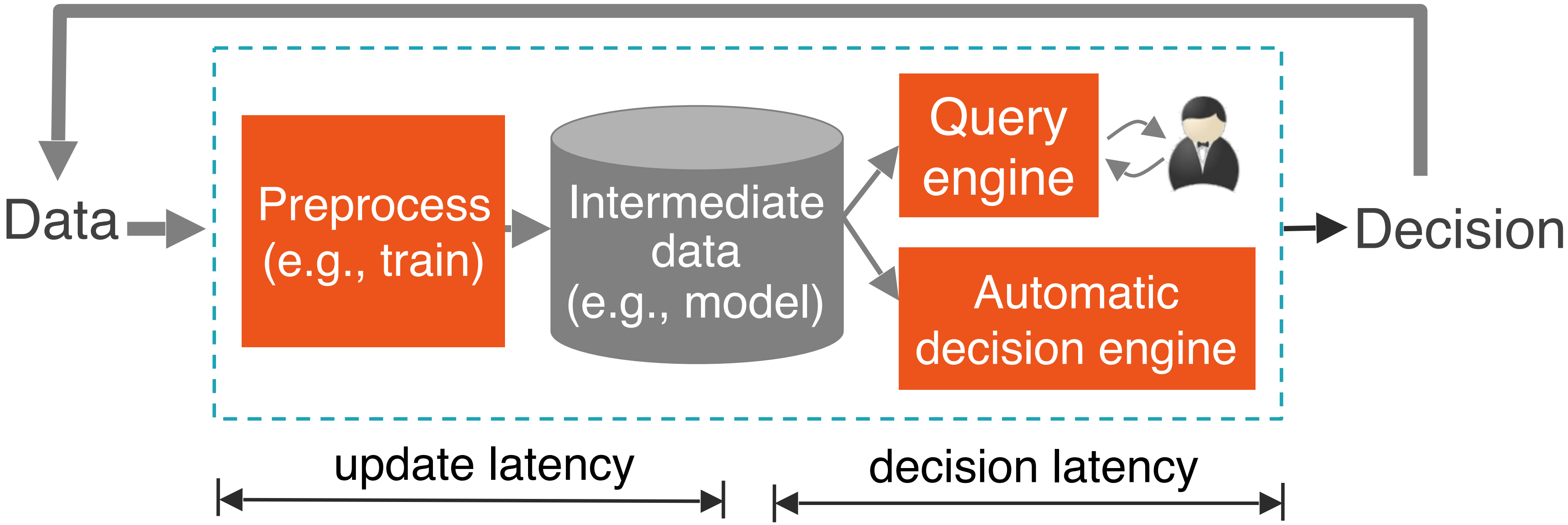
What does this mean?

- Faster decisions better than slower decisions
- Decisions on fresh data better than decisions on stale data
- Decisions on personalized data better than on generic data

Goal

Real-time decisions	*decide in ms*
on live data	*the current state of the environment*
with strong security	*privacy, confidentiality, integrity*

Typical decision system



Want low update latency & low decision latency

Why is it hard?

Want high **quality** decisions

- Sophisticated, e.g., fraud, forecast, fleet of drones
- Accuracy, low false positives and negatives
- Robust to noisy and unforseen data

Want low **latency** for both updates and decisions

Want strong **security**: privacy, confidential, integrity

Example: Zero-time defense

Problem: zero-day attacks can compromise millions of hosts in seconds

Solution: analyze network flows to detect attacks and patch hosts/software in real-time

- **Intermediate data**: create attack model
- **Decision**: detect attack, patch

Quality	sophisticated, accurate, robust
Latency	update (sec) / decision (ms)
Security	privacy (encourage users to share logs), integrity

Application	Quality	Latency		Security
		Update	Decision	
Zero-time defense	sophisticated, accurate, robust	$\boxed{\text{sec}}$	ms	privacy, integrity
Parking assistant	sophisticated, robust	sec	sec	privacy
Disease discovery	sophisticated, accurate	hours	sec/min	privacy, integrity
IoT (smart buildings)	sophisticated, robust	min/hour	sec	privacy, integrity
Earthquake warning	sophisticated, accurate, robust	min	$\boxed{\text{ms}}$	integrity
Chip manufacturing	sophisticated, accurate, robust	min	sec/min	confidentiality, integrity
Fraud detection	sophisticated, accurate	min	ms	privacy, integrity
“Fleet” driving	sophisticated, accurate, robust	sec	sec	privacy, integrity
Virtual companion	sophisticated, robust	min/hour	sec	integrity
Video QoS at scale	sophisticated	min	ms/sec	privacy, integrity

Challenges	RISE Lab
Automated decisions on live data are hard	Real-time, sophisticated decisions that guarantee worst-case behavior on noisy and unforseen live data
Poor security: exploits are daily occurrences	Ensure privacy and integrity without impacting functionality
One-off solutions, expensive, slow to build	General platform: **Secure Real-time Decision Stack**

Research directions

Systems: 100x lower latency, 1,000x higher concurrency than today's Spark

Machine learning: Robust, on-line ML algorithms

Security: achieve privacy, confidentiality, and integrity without impacting performance or functionality

Early work

Drizzle

Opaque

Streaming

Micro-batching vs. record-at-a-time

Micro-batching (e.g., Spark) inherits batch's properties

- fault-tolerance
- straggler mitigation
- optimizations
- unification with other libraries

Record-at-a-time (e.g., Storm, Flink), typically lower latency

Yahoo's streaming benchmark

Input: 20M JSON ad-events / second, 100 campaigns

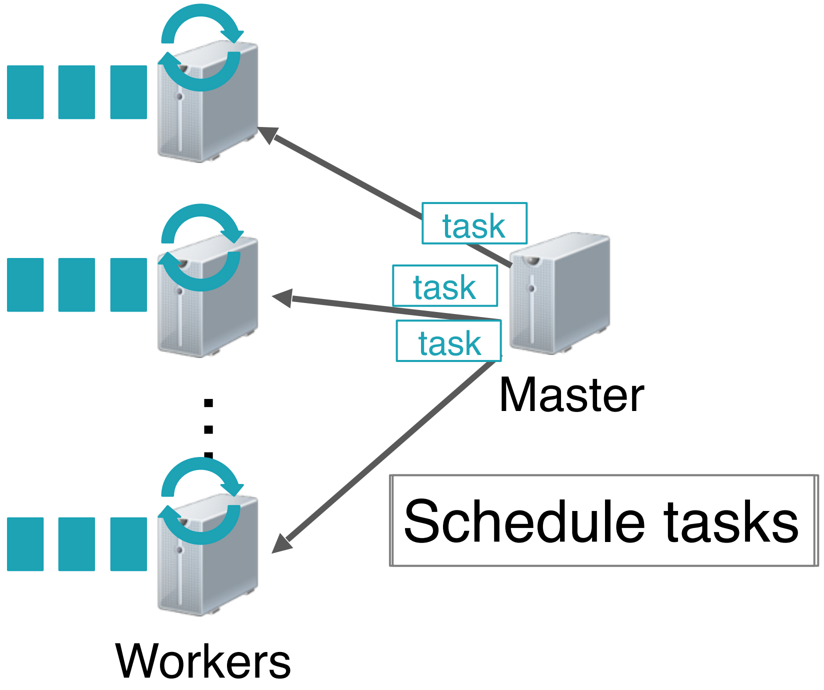
Output: ad counts per campaign over a 10sec window

Latency: (end of window) – (time last event was processed)

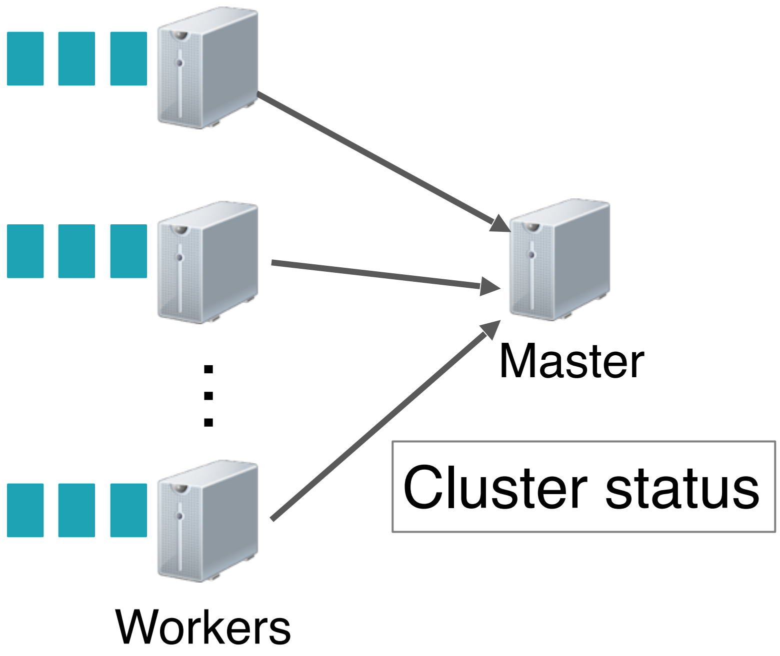
SLA: 1sec

Findings: Storm, Flink provide indeed lower latency than Spark

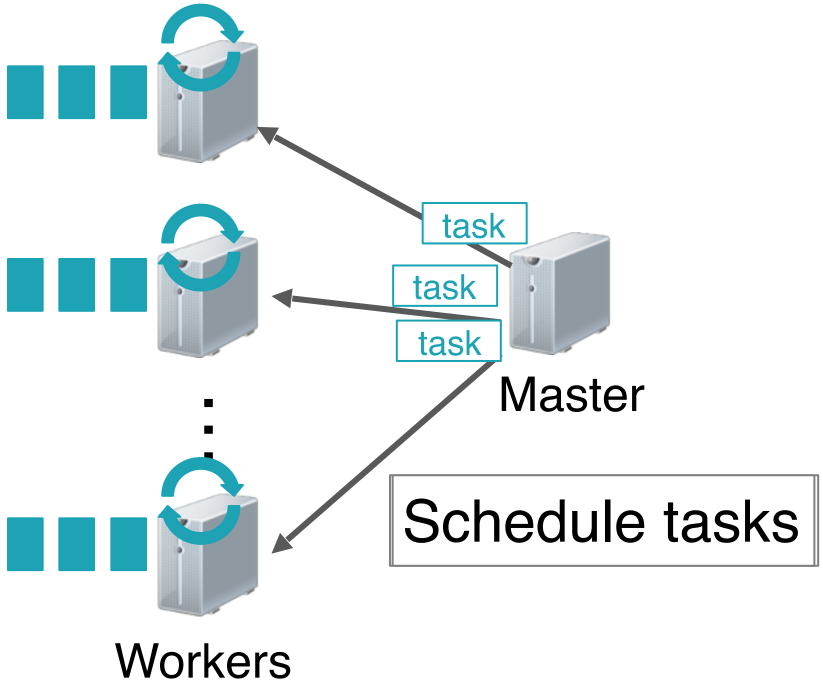
Spark Streaming



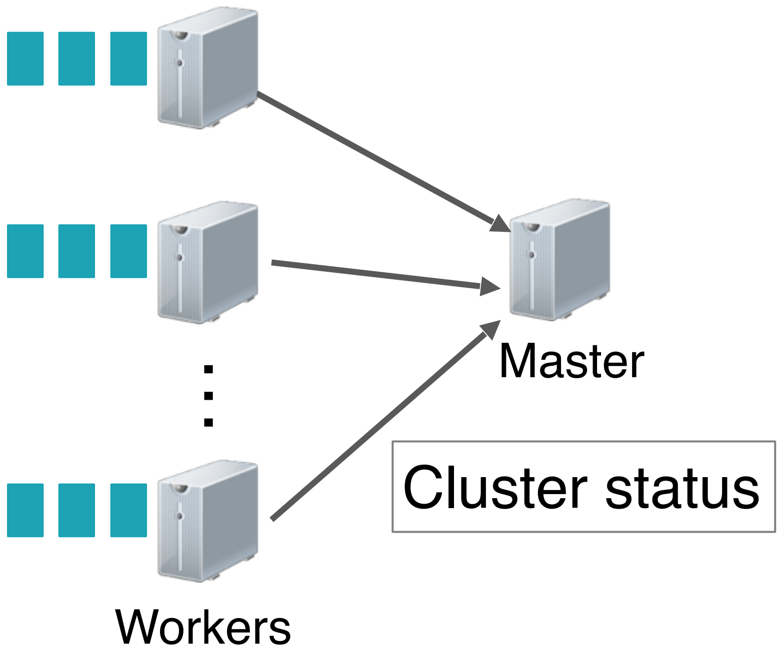
Spark Streaming



Spark Streaming



Spark Streaming



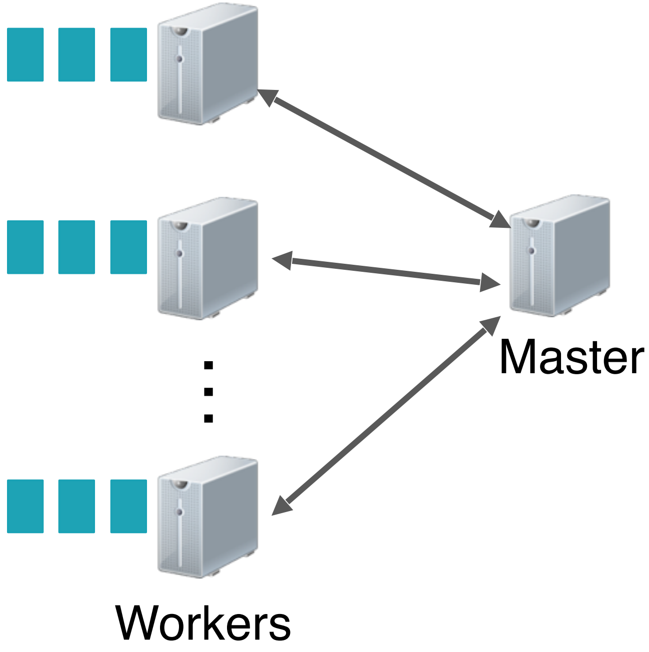
Drizzle

Goal: reduce Spark streaming latency by at least 10x

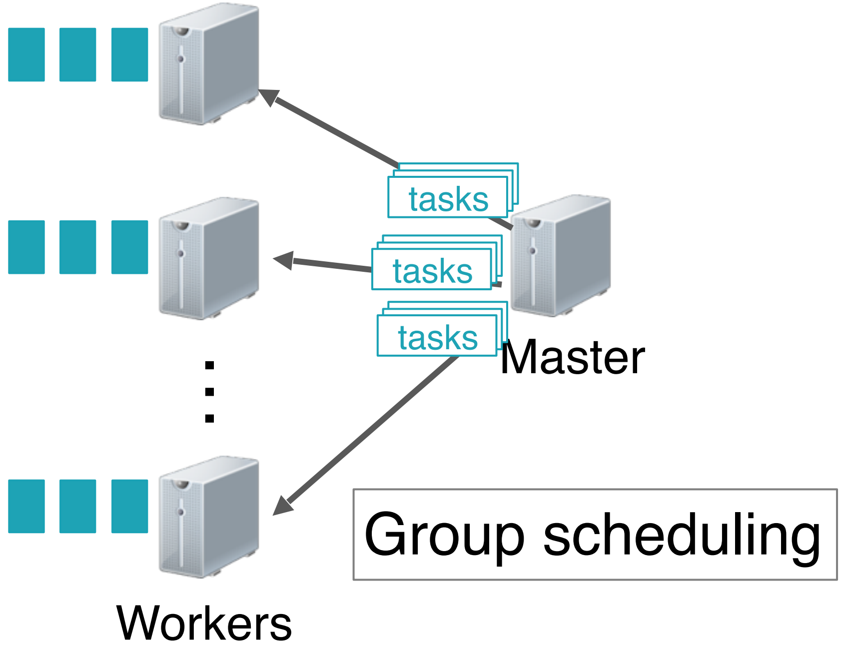
Key observation: consecutive iterations use same DAG

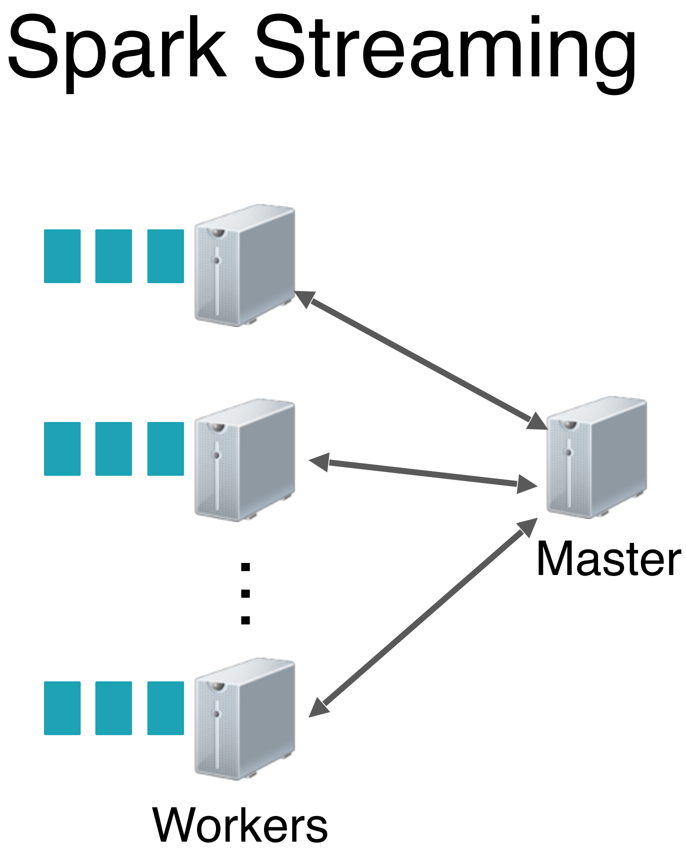
Solution: push scheduling decisions to workers

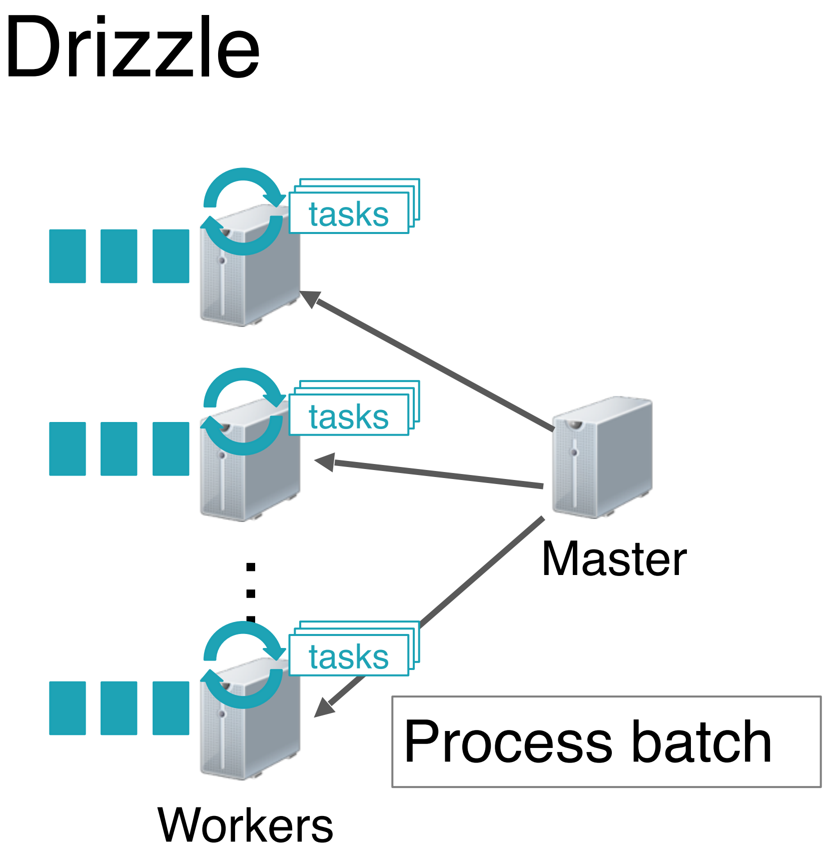
Spark Streaming



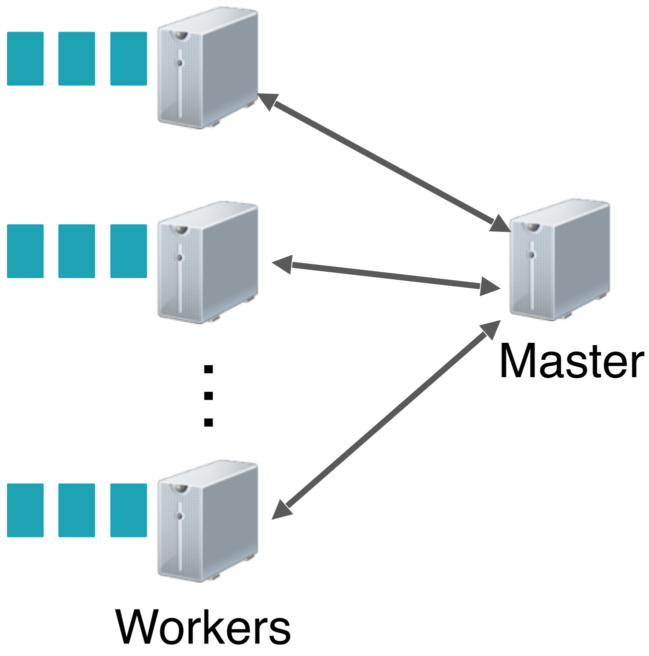
Drizzle



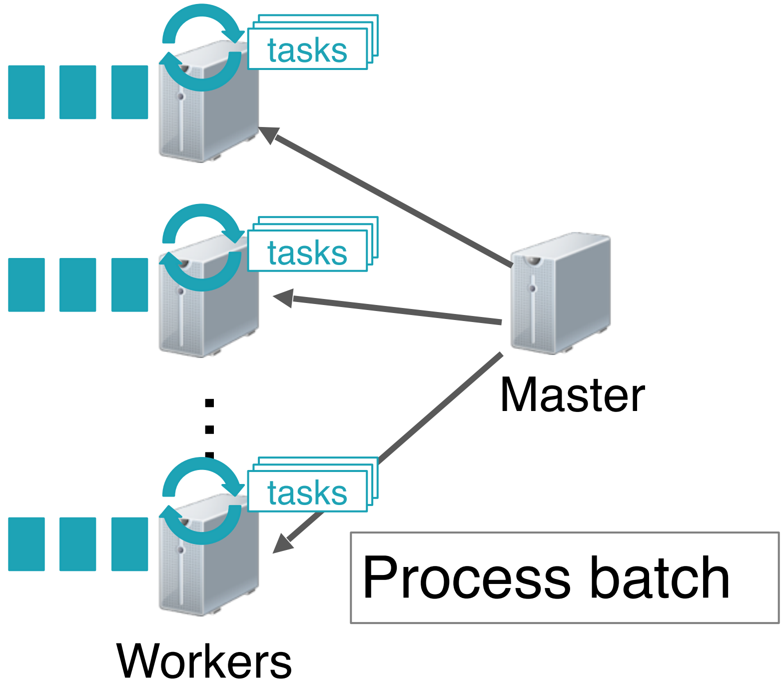

Spark Streaming
Master
Workers


Drizzle
tasks
tasks
tasks
Master
Process batch
Workers

Spark Streaming

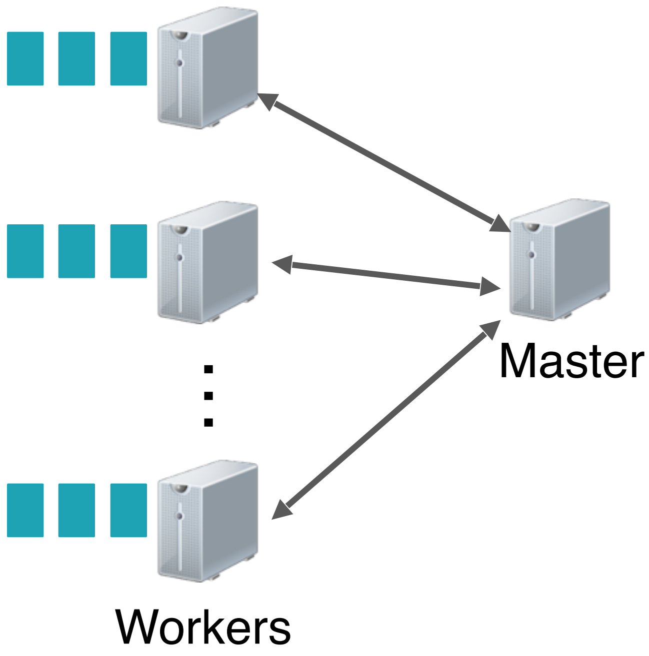


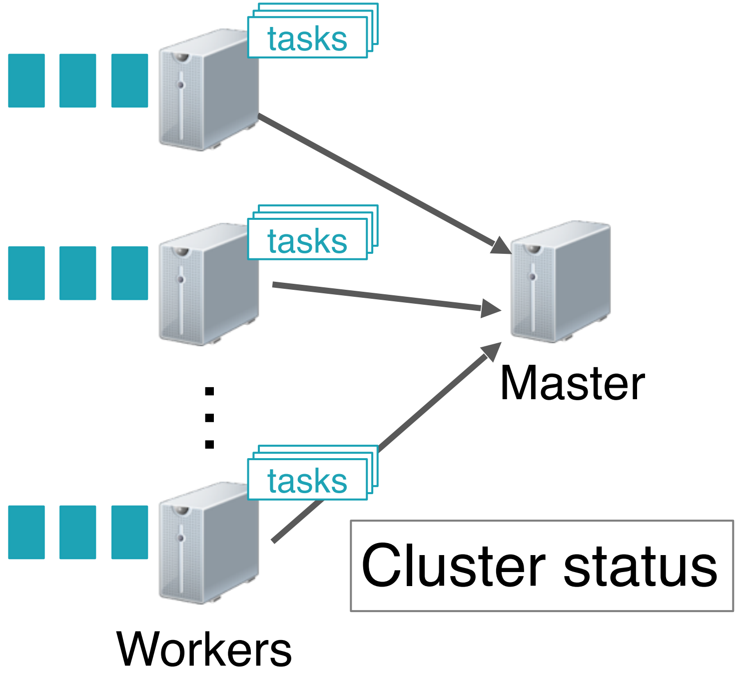
Drizzle



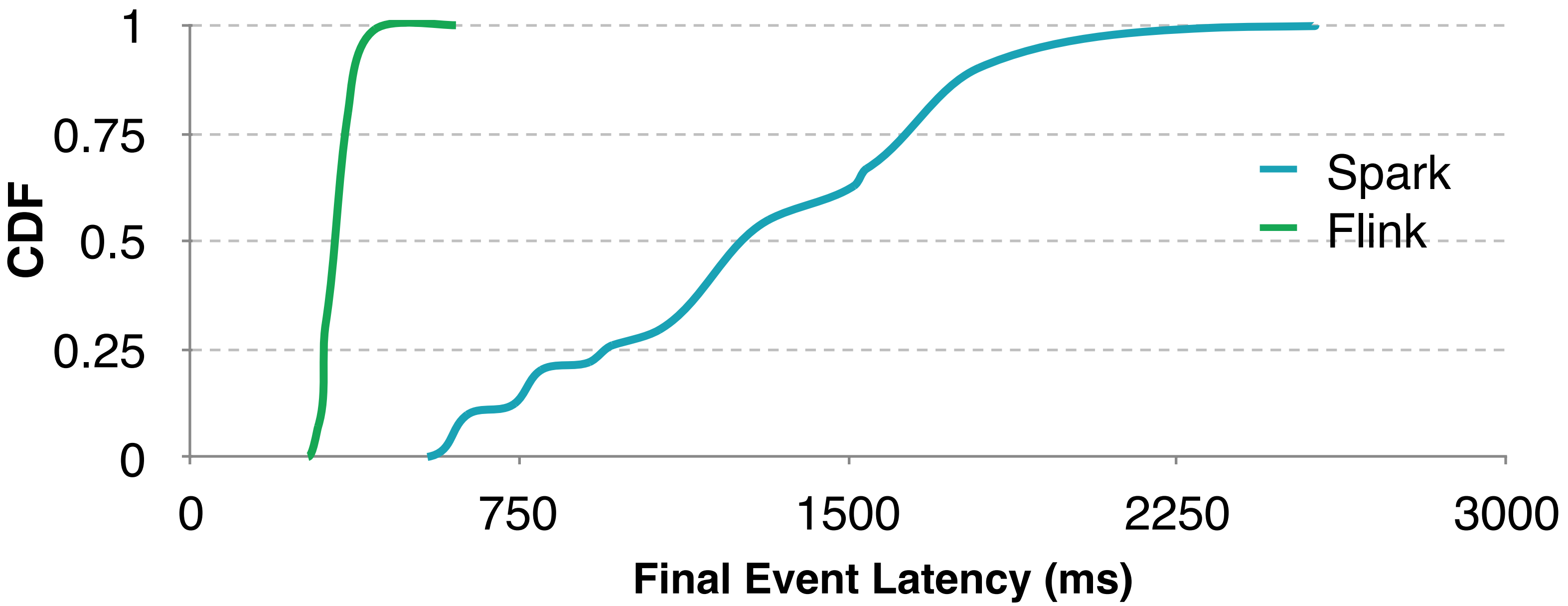
Spark Streaming

Drizzle



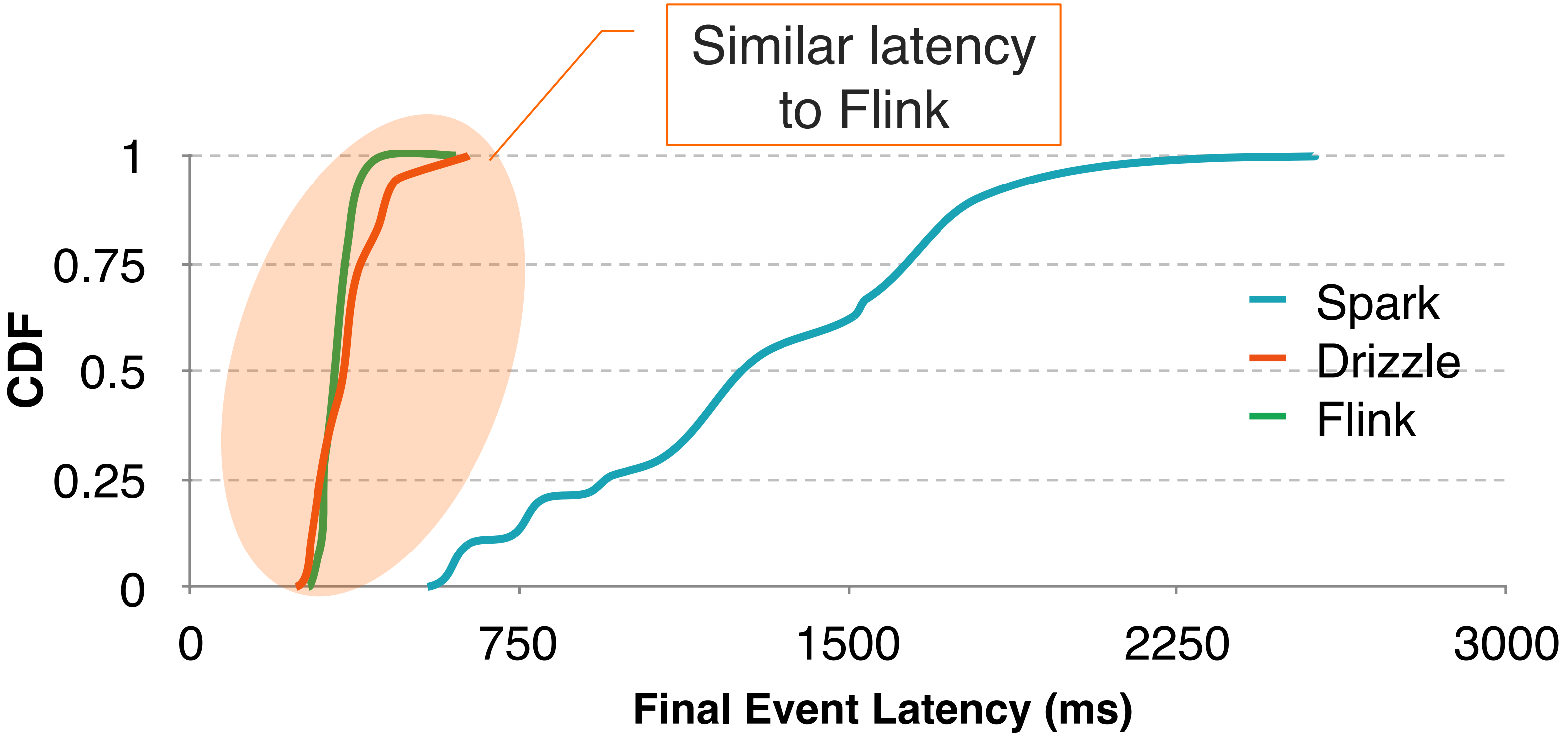


Latency

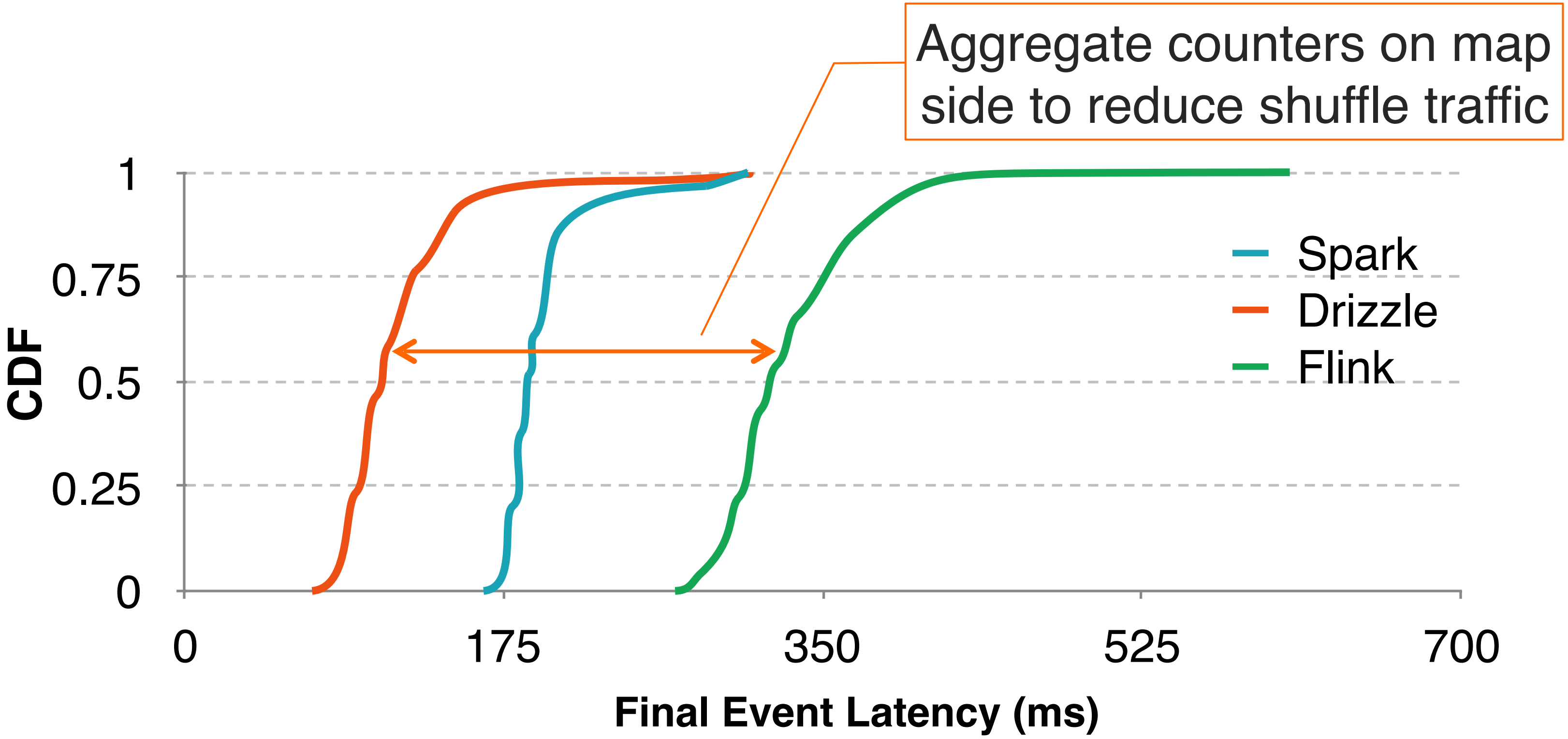


1
0.75
0.5
0.25
0
CDF
0
750
1500
2250
3000
Final Event Latency (ms)
Spark
Flink

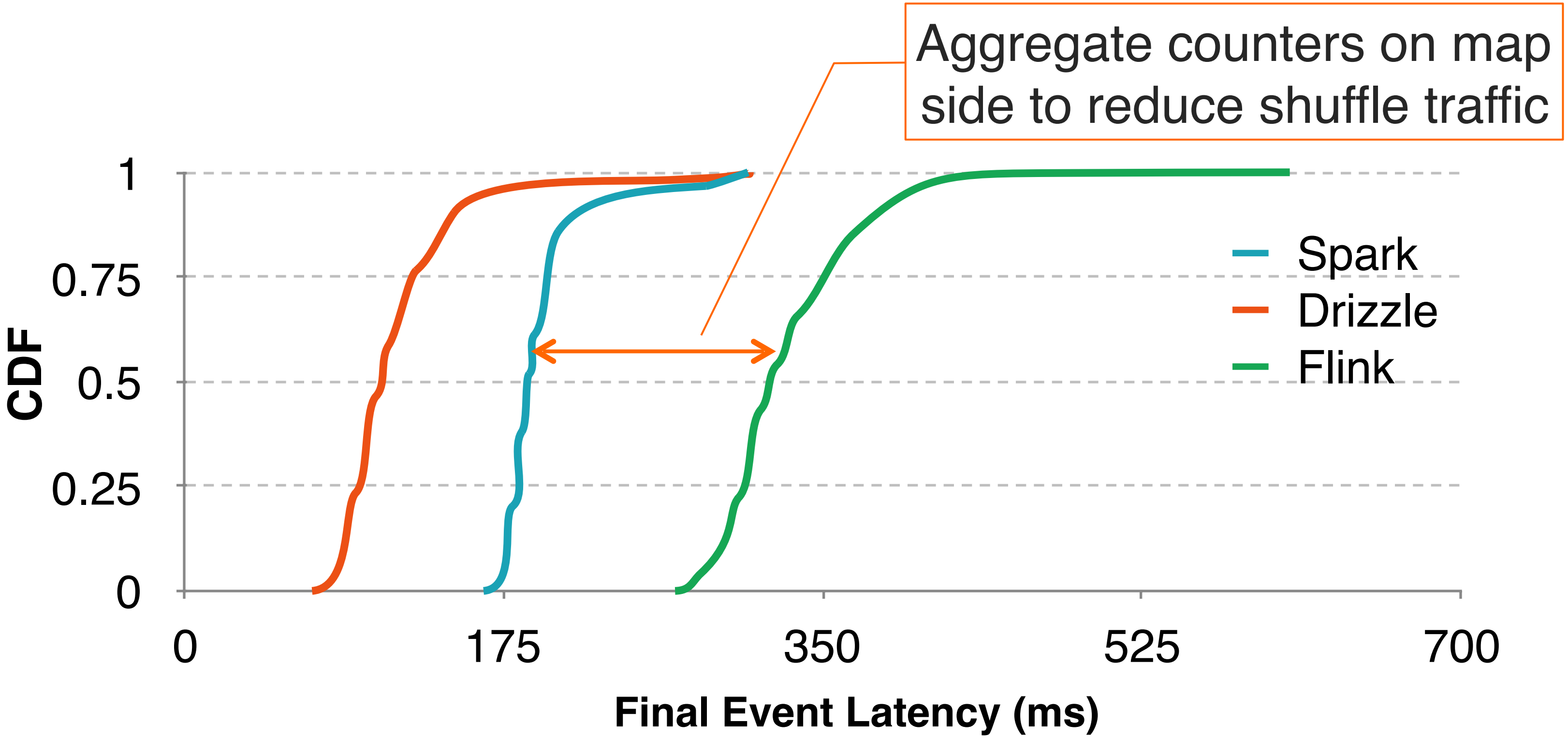
Latency


Similar latency
to Flink
1
0.75
0.5
0.25
0
CDF
0
750
1500
2250
3000
Final Event Latency (ms)
Spark
Drizzle
Flink

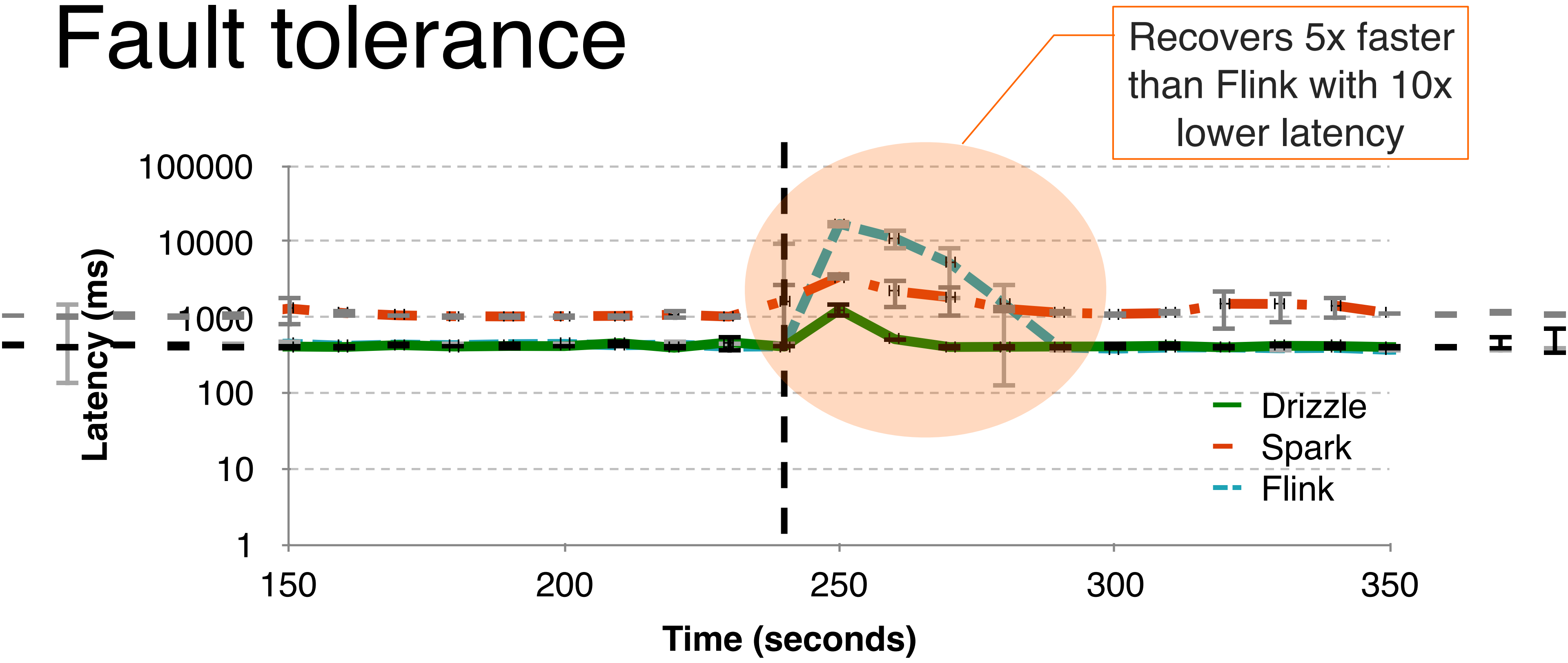
Latency, w/ ReduceBy optimization



Latency, w/ ReduceBy optimization



Fault tolerance



four nines SLA: 8.6 sec per day exceeding SLA

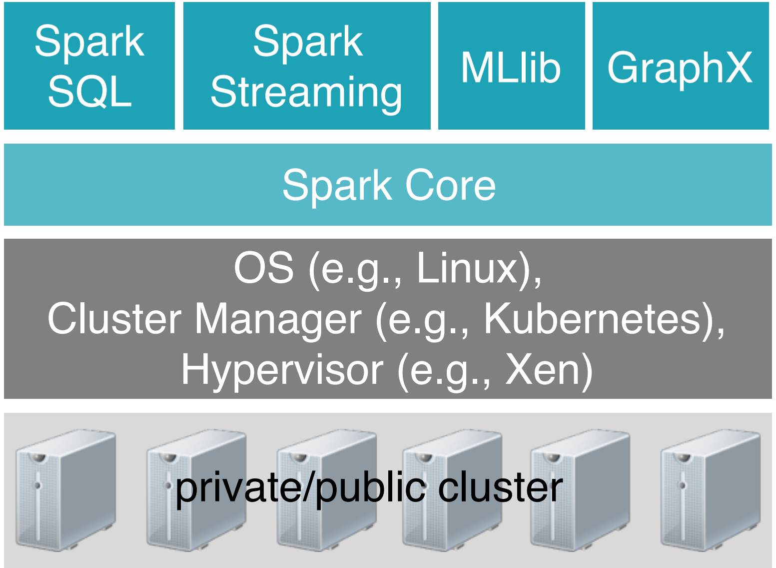
Early results

Drizzle

Opaque

State-of-the-art security today

Authentication, encryption at-rest and in-motion

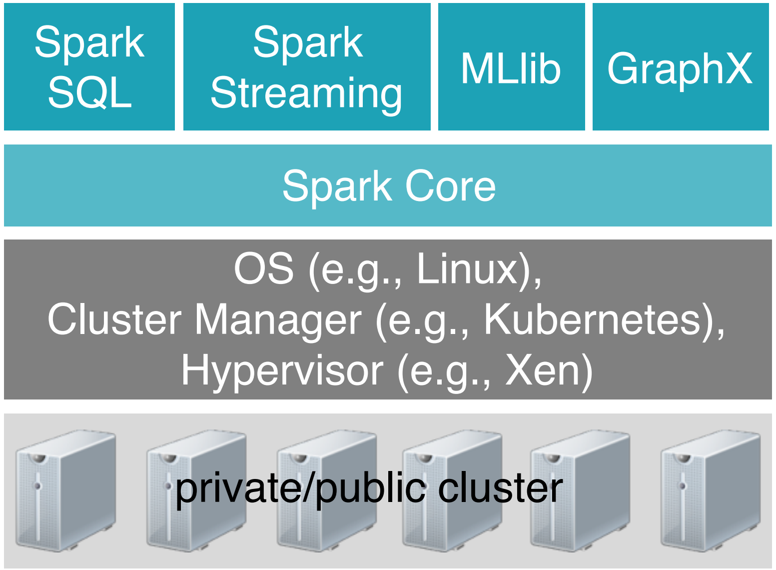


Not enough if OS or hypervisor compromised, and attacker get root access

databricks

State-of-the-art security today

Authentication, encryption at-rest and in-motion

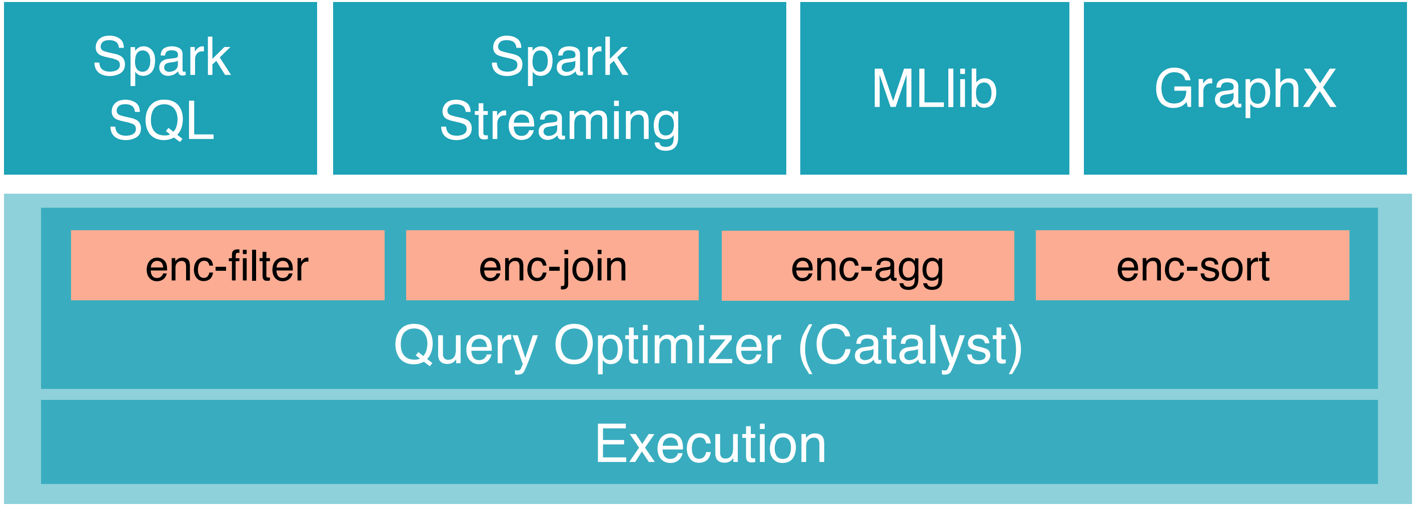


Not enough if attacker can observe network and memory access patters

Opaque

Leverage Intel's SGX: hardware enclave

Implement secure distributed relational algebra



Opaque: two modes

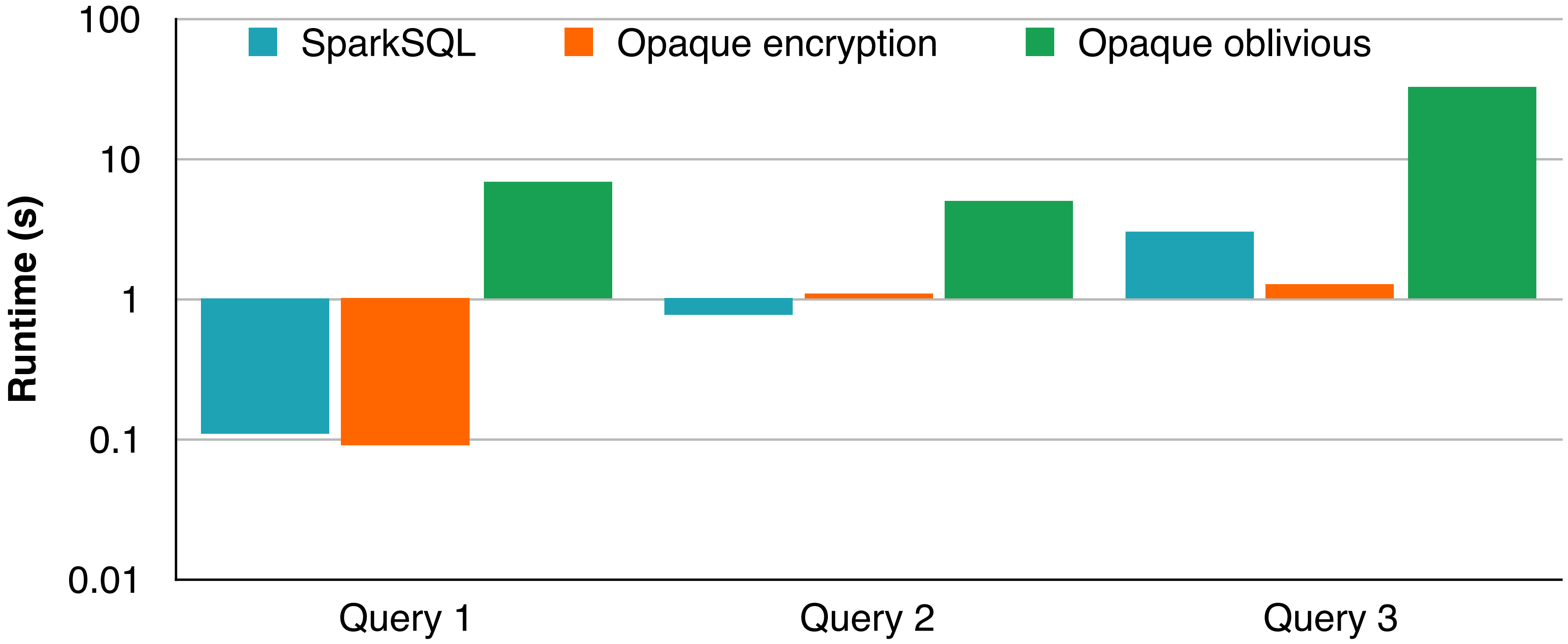
Encryption mode

- Protect against compromised software (e.g., OS)
- Full data encryption, authentication, and computation verification in hardware enclave

Oblivious mode

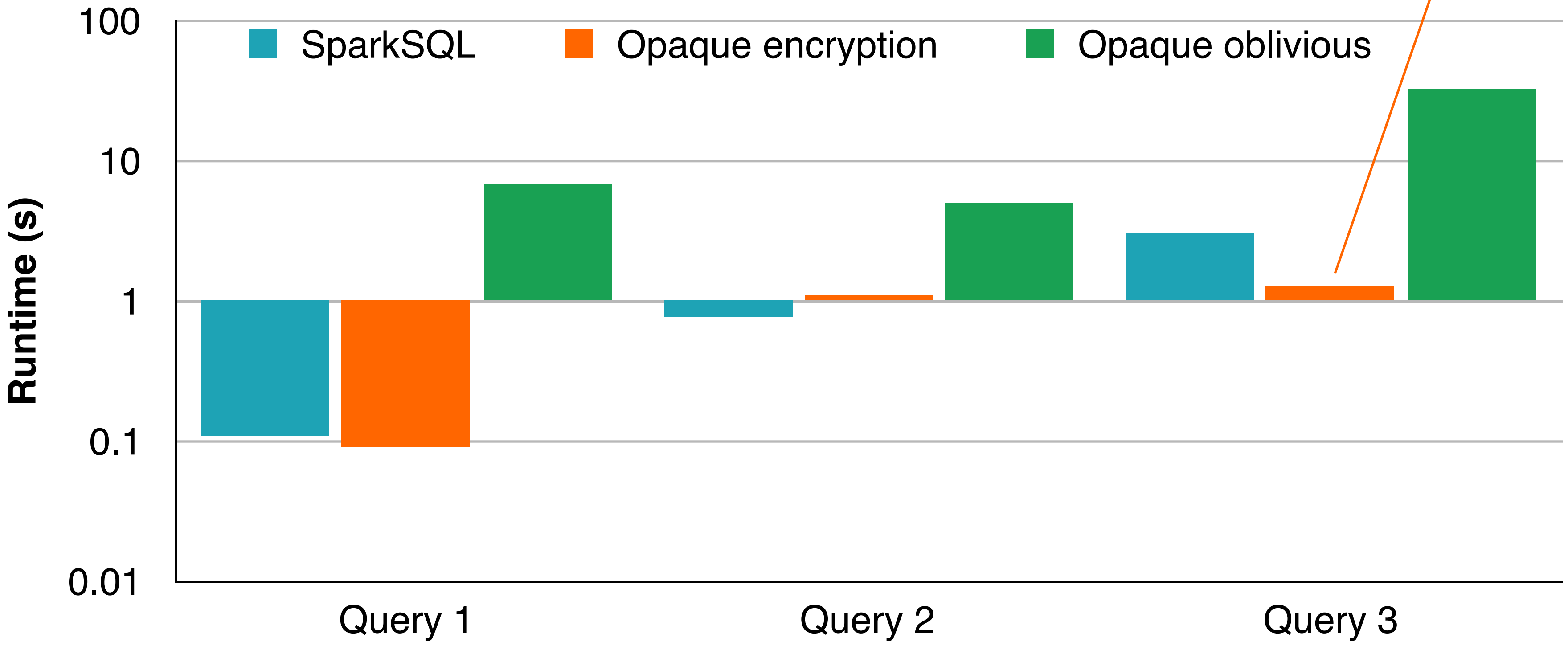
- Additionally, hide data access pattern

Opaque: Big Data Benchmark



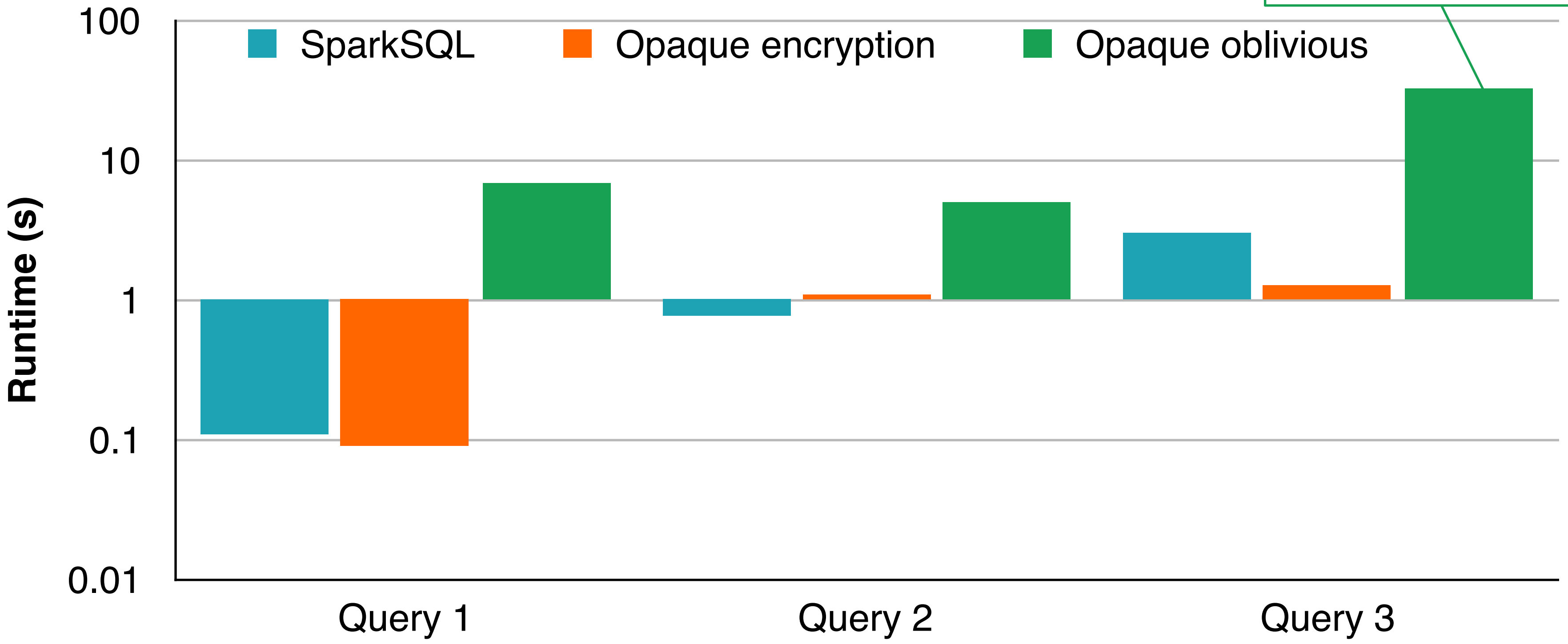
Opaque: Big Data Benchmark

Encrypted operators implemented in C++



Opaque: Big Data Benchmark

Up to 100x slower but 1,000x faster than state-of-the-art



Next AMPLab: RISELab

Goal: develop Secure Real-time Decision Stack, an open source platform, tools and algorithms for real-time decisions on live data with strong security

Already promising results

Expect much more over the next five years!

Thank you

databricks

AMPLab alumni presenting here





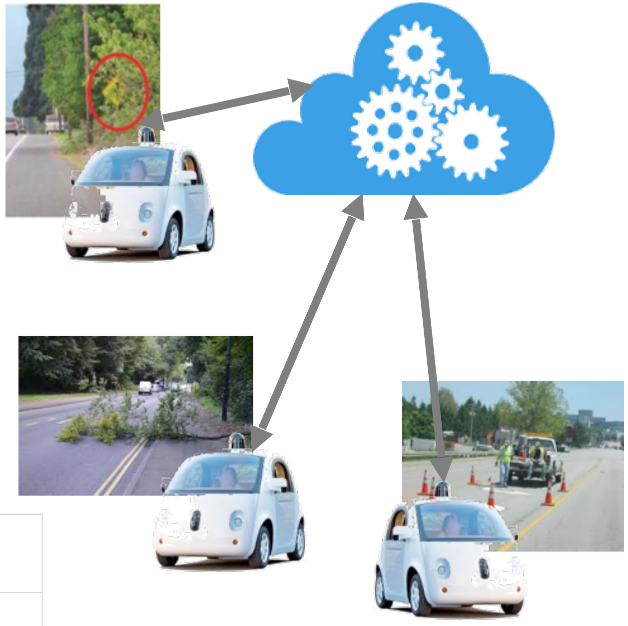



Example: “Fleet” driving

Problem: suboptimal driving decisions

Solution: collect & leverage info from other cars and drivers in real-time

- **Intermediate data**: automatically annotate maps, actions of other drivers
- **Decision**: avoid obstacles, congestions



Quality	sophisticated, accurate, noise tolerant
Performance	sec (decision) / sec (update)
Security	privacy, data integrity

Not only hypothetical

Attacks getting root access by exploiting OS/DBs vulnerabilities

THE WALL STREET JOURNAL.

BUSINESS

Anthem: Hacked Database Included 78.8 Million People

Health insurer says data breach affected up to 70 million Anthem members

InformationWeek DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

Conficker Showdown: No End In Sight

Reinfected machines likely part of the 5.5 to 6 million-strong Conficker headcount

COMPUTERWORLD FROM IDG

NEWS

Hackers gain root access to WordPress servers

Attacks exploiting access pattern leakages

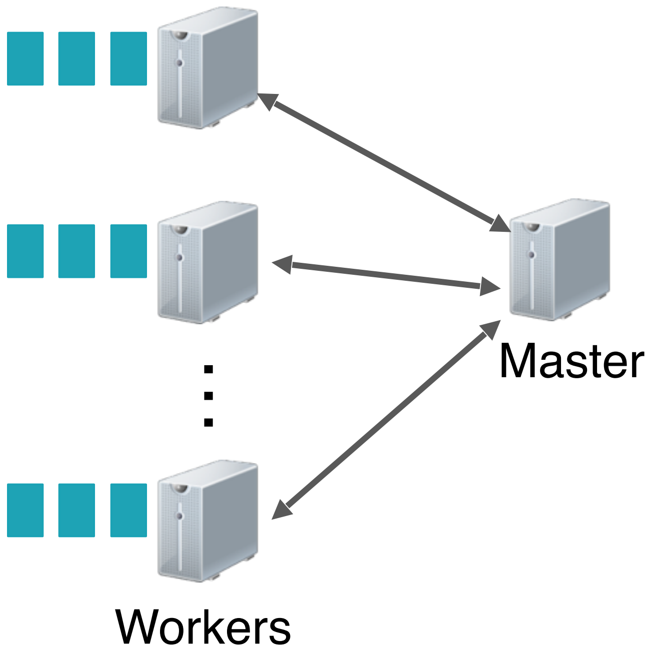
Observing and Preventing Leakage in MapReduce*

Olga Ohrimenko, Microsoft Research, oohrim@microsoft.com
Manuel Costa, Microsoft Research, manuelc@microsoft.com
Cédric Fournet, Microsoft Research, fournet@microsoft.com
Christos Gkantsidis, Microsoft Research, christos.gkantsidis@microsoft.com
Markulf Kohlweiss, Microsoft Research, markulf@microsoft.com
Divya Sharma†, Carnegie Mellon University, divyasharma@cmu.edu

Controlled-Channel Attacks: Deterministic Side Channels for Untrusted Operating Systems

Yuanzhong Xu, *The University of Texas at Austin*, *yxu@cs.utexas.edu*
Weidong Cui, *Microsoft Research*, *wdcui@microsoft.com*
Marcus Peinado, *Microsoft Research*, *marcuspe@microsoft.com*

Spark Streaming



Drizzle