AEROSPIKE NEXT GEN NOW SUMMIT '20

Preventing Fraud @ Grab

Grab

Raghavendra Nagaraj
PRINCIPAL ENGINEER,
RISK & COMPLIANCE
GRAB

Srinivas Chamarthy
HEAD OF ENGINEERING,
MERCHANT PAYMENTS, RISK & COMPLIANCE
GRAB

Preventing Fraud @Grab

- Grab is one of the most popular superapp in SE Asia and has a huge presence in payments - Taxi, Food, Wallet, P2P, P2M, Online Acceptance, Lending, Insurance, Wealth.
- Bad actors at play, Fraud attacks - using stolen cards, rewards gaming, AML, P2M collusion.
- Potential loss of millions of dollars due to chargebacks, legal and reputational harm, potential loss of wallet licence, fines, user trust loss.
- Built an in-house fraud service

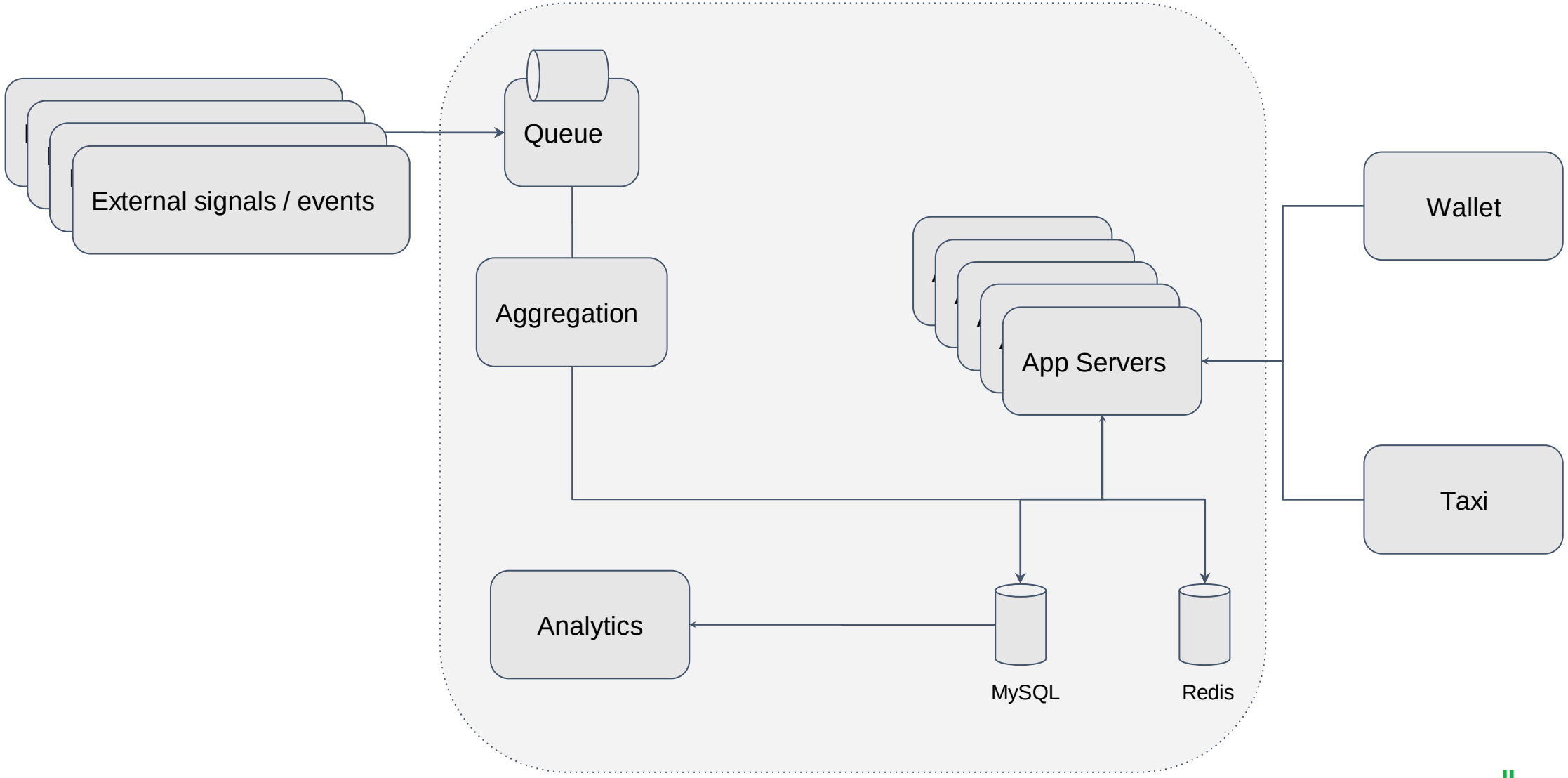
Grab Fraud Service

- Used across Grab for all platforms and micro-services
  - Listens to all verticals and systems for events that are processed
- Rules engine and Aggregations as a service
- Real Time rule editor:
  - Velocity rules - Counts and Amounts over various time windows
  - ML Models - Supervised classification
  - Static features like 3DS responses from Gateways, BIN
  - Device level verdicts
  - Location based rules

Benefits

- Customer
  - Increased user trust
- Safeguards
  - Reputational harm / bad press
  - Legal actions and fines
  - Card scheme actions
  - Fraudulent gaming of rewards
- Cost savings
  - Vendor cost
  - Chargebacks

Where we were...

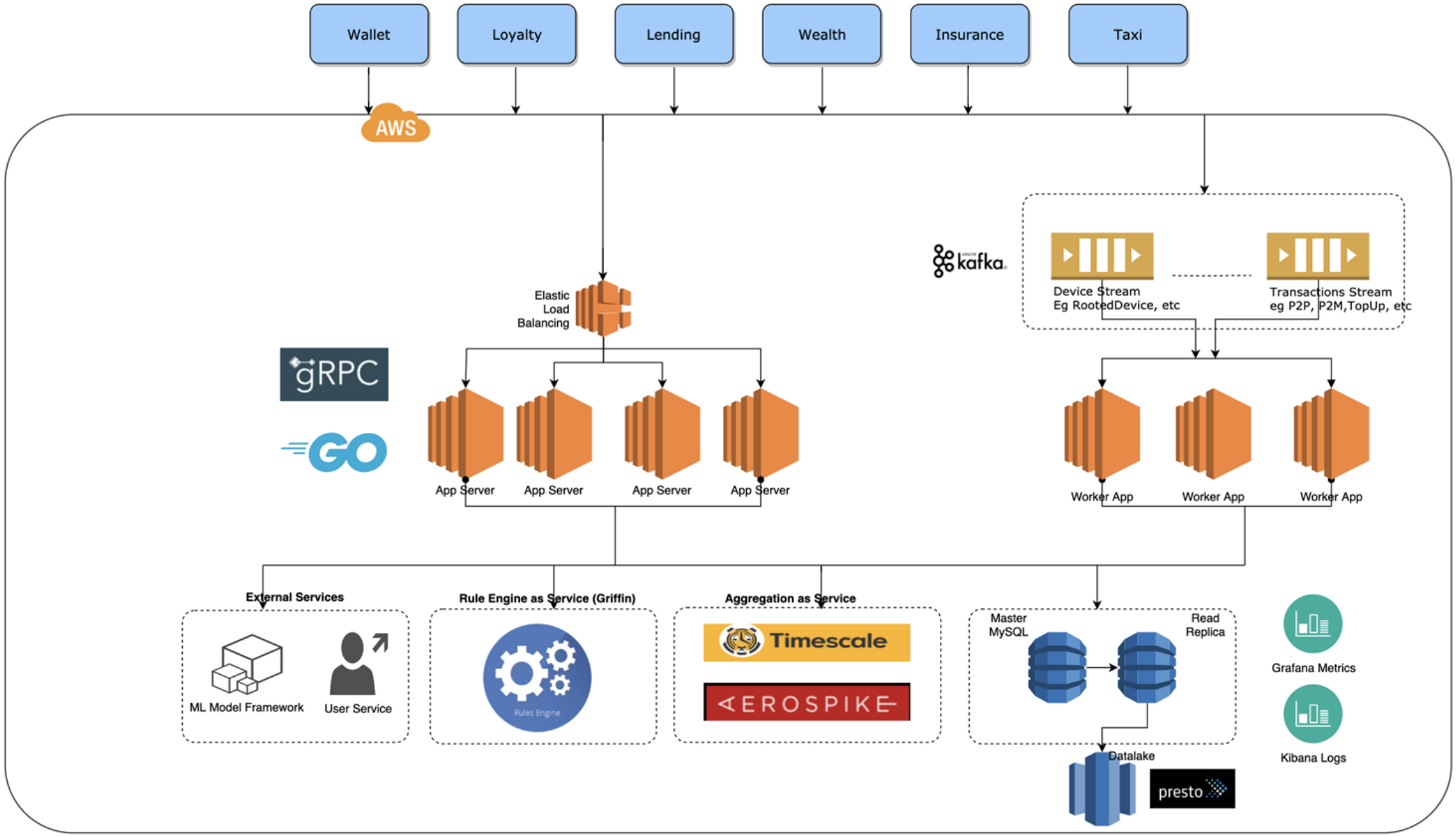


Challenges

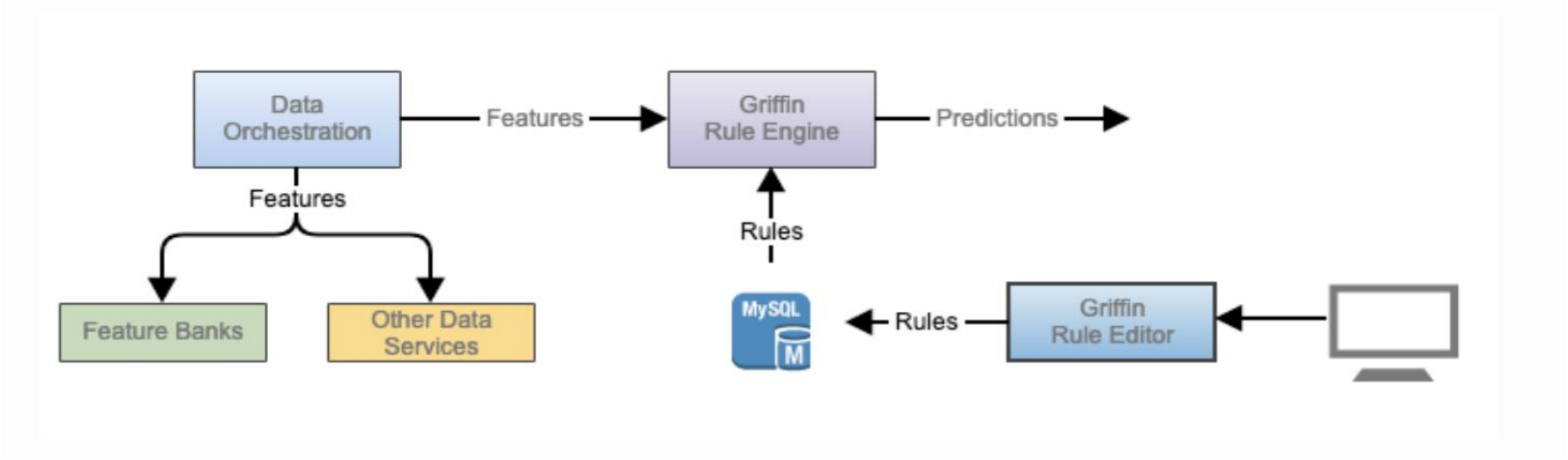
List of issues in the old architecture that prompted us to go for the change:

- Scale
- Adaptability
- Maintenance
- GTM
- Storage costs
- Tech challenges

2.0


Wallet
Loyalty
Lending
Wealth
Insurance
Taxi
AWS
kafka
Device Stream
Eg RootedDevice, etc
Transactions Stream
eg P2P, P2M,TopUp, etc
Elastic
Load
Balancing
gRPC
GO
App Server
App Server
App Server
App Server
Worker App
Worker App
Worker App
External Services
ML Model Framework
User Service
Rule Engine as Service (Griffin)
Rules Engine
Aggregation as Service
Timescale
EROSPIKE
Master
MySQL
Read
Replica
Grafana Metrics
Kibana Logs
Datalake
presto

Griffin - Rules Engine



d.sender.authenticated_response_3ds == "Y" and d.sender.offered_response_3ds == "Y" and d.transaction.amount > 100

Aggregations as a Service

- Listens to any stream and aggregates - Transactions stream and Device stream

- Complex Aggregations based on time windows
  - How many transactions were done by a user in last x mins/hours/days/months

- Various combinations of P2P, P2M
- Short lived aggregates on TimescaleDB (built on PostgreSQL)
- Longer lived aggregates on Aerospike

TimescaleDB

- An open-source database built for analyzing time-series data with the convenience of SQL and reliability of PostgreSQL
- Has built-in tools to perform common time-series data analysis, including buckets, gap filling, aggregations and more
- Achieves faster ingest and query rates by automated time-space partitioning by providing an abstraction called hypertable

Aerospike

- Used to store aggregates for larger time windows - daily, monthly, yearly and lifetime
- Using nested maps and atomic map increment operations
- Using Hybrid Memory Architecture
- Using Aerospike version 4.5 Enterprise edition

Key: 12345.98765.success.SGD (format - from.to.status.currency)

Record:

```
{
    “200401”: {“a”: 400, “c”: 20}, // 2020-04-01
    “2004”: {“a”: 5000, “c”: 122}, // 2020-04
    “lifetime”: {“a”: 20000, “c”: 302}
}
```

Thank You