

Final Presentation

August 5, 2024

GabbleGrid

To reduce the growing impact of service outages by developing a system of autonomous AI Agents that enhances service resiliency

How one flawed software update could have such widespread effects — and cost "potentially billions of dollars"

From CNN's Brian Fung

Global tech outage disrupts airlines, banks, hospitals, 911 services

TECHNOLOGY

Major Tech Outage Grounds Flights, Hits Banks and Businesses Worldwide

CrowdStrike update causes device outages for millions of Microsoft Windows users

By Sam Schechner, Gareth Viper and Alyssa Lukpat

Updated July 19, 2024 1:51 pm ET

Share, Save, Listen (9 min)



An update from cybersecurity software company CrowdStrike caused outages for millions of Microsoft Windows devices.

A major IT outage left businesses and financial firms across the world unable to access computing systems. Several airlines and airports reported disruptions which led to canceled flights. PHOTO: JOSÉ SARMENTO MATOS/WSJ

A massive tech outage swept the globe, knocking out operations for banks, media companies and emergency services and forcing airlines to ground flights.

Travel snarls



airport in Hambu



could be the 'largest IT outage in history,' an expert says. Recovering from it is expected to

This could be the 'largest IT outage in history,' an expert says. Recovering from it is expected to be a long, arduous process.

32 minutes ago Jill Cowan

Portland's mayor, Ted Wheeler, [declared a city emergency early on Friday morning](#) after some of the city's computer systems, including ones used in 911 dispatch operations, crashed as a result of the CrowdStrike outages. City officials emphasized that emergency dispatch services went back to normal by about 6 a.m. on Friday, and city services continued throughout the morning, but residents should expect delays in getting non-emergency calls answered.

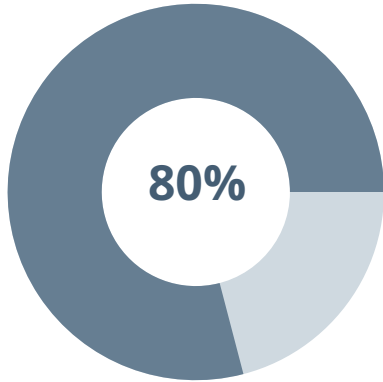
We are team GabbleGrid

We focus on Service Outages in complex IT
Infrastructure

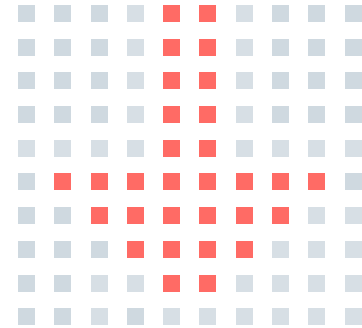
Service Outage is an unplanned
downtime resulting in service
disruption

It can occur for reasons like human error,
technical issues, cyberattacks etc

How Often do Service Outages Occur?

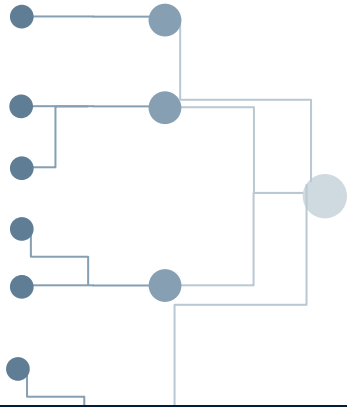


of organizations have experienced an outage in the last 3 years.



> 30%: of outages result in a direct revenue loss.

IT Admin | Concerns



1

Unsure which ML model to choose and how to evaluate them.

2

Needs help with selecting and automating actions.

ACTION



LOGS

Hardware Data

Software Data

Environment Data

Network Data

Security Data

Maintenance Data

External Data

Answer



Self-Healing Clouds with AI Agents

Welcome, Gaurav Narasimhan!

[Login with GitHub](#) [Login with Google](#)

Needs help with selecting and automating actions.

2

Is a platform for Deploying Teams of Agents

1

Is a platform for Model Selection & Evaluation

Unsure which ML model to choose and how to evaluate them.

LOGS

Hardware Data

Software Data

Environment Data

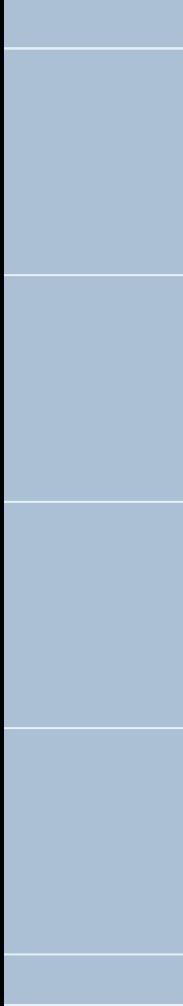
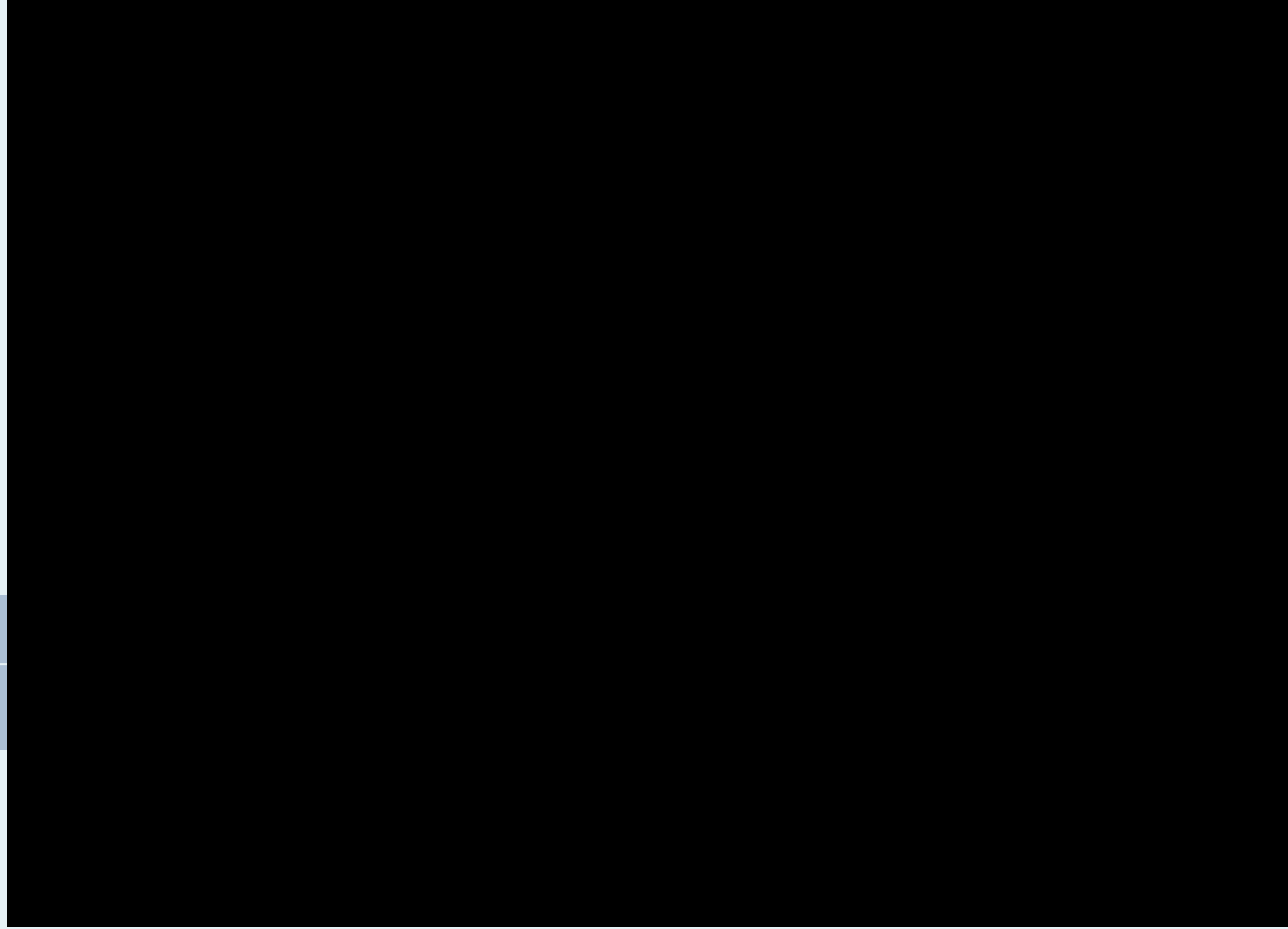
Network Data

Security Data

Maintenance Data

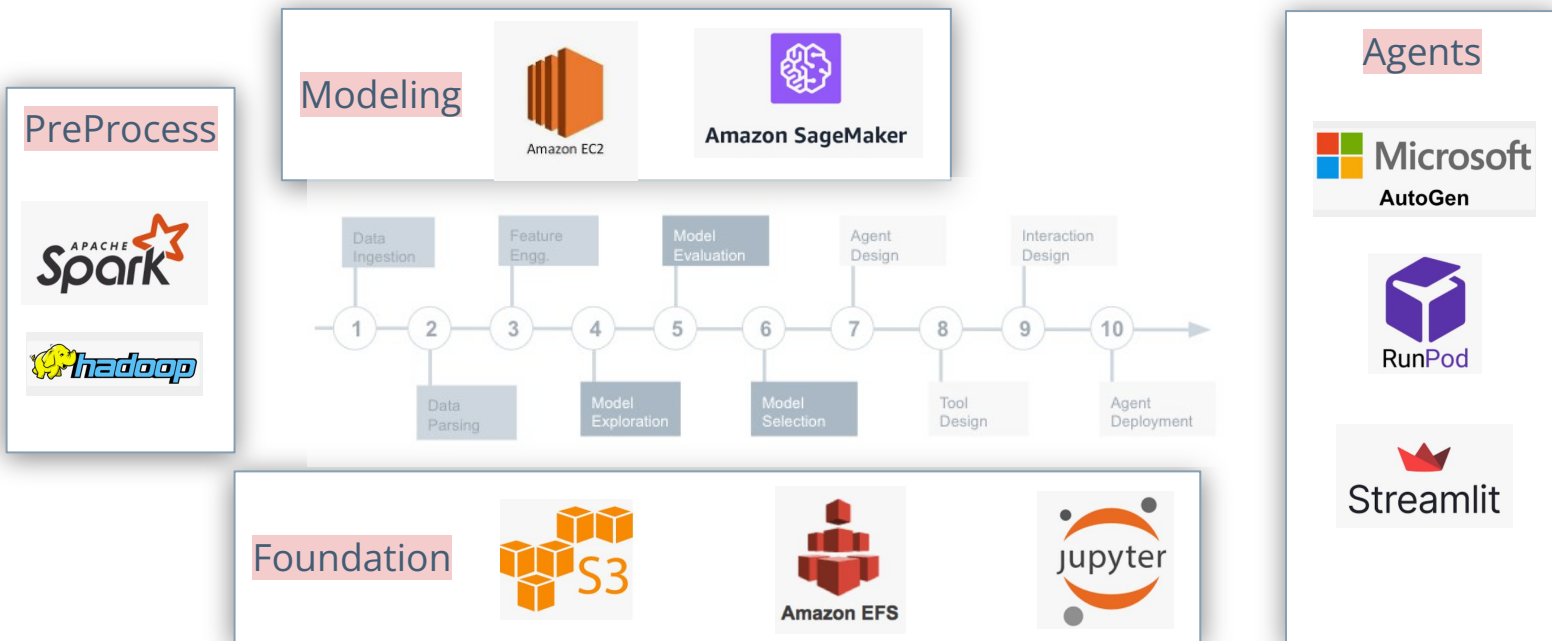
External Data

Demo



System Components

The core infrastructure was hand-crafted on ec2 instances



Agent Teams

Runs Model Inference and generates email based on analysis

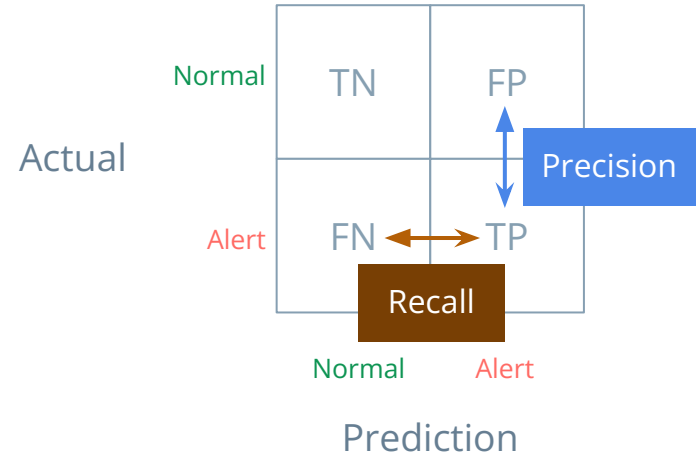


Critical Factor | Precision vs Recall

Key Insight: False Positives lead to significant disruption & resource wastage

Stakeholder Feedback

1. **Reducing false positives** ensures that alerts are more actionable and **reliable**
2. **High precision** helps maintain **trust** in the alerting system, so when an alert is raised, it is likely to be a true anomaly



Base Model | Transformers

Encoder Only Model with Classification head

Encoder-Only Transformer

- Uses only the encoder for processing sequential log data

Embedding and Positional Encoding

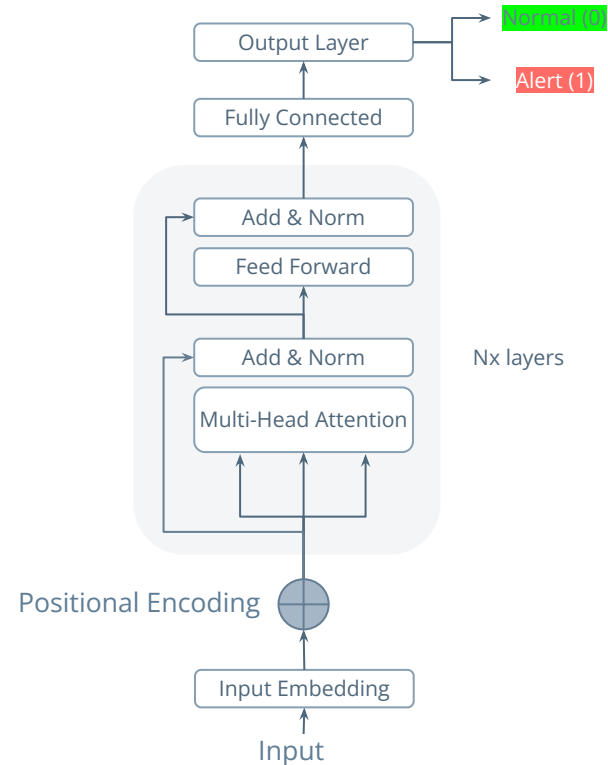
- Transforms logs into high-dimensional embeddings with positional information.

Classification Head

- Fully connected layer with sigmoid activation for binary classification.

Binary Output

- Outputs probability thresholded to classify logs as normal (0) or anomalous (1).



Learnings

Log data is unstructured, messy and unreliable

Model performance is average, but is a great foundation to build on

Underestimated the scale and complexity of the problem

Relatively light amount of research and precedent → reverted to first principles



Roadmap

Expand Scope
from BG/L to
ThunderBird etc



Use more features in
the GabbleGrid app;
add visualizations

Improve Model
Robustness with
focus on Precision

Mission

To **reduce** the growing impact of **service outages** by developing a **system of autonomous AI Agents** that enhances service **resiliency**

THANKS!

Do you have any questions?

gaurav.narasimhan@berkeley.edu
efemson_01@berkeley.edu

CREDITS: This presentation template was created by [Slidesgo](#), and includes icons by [Flaticon](#), and infographics & images by [Freepik](#)