



GOPS 2021  
Shenzhen

# GOPS

# 全球运维大会

2021  
-XOPS 风向标



深圳站

中国·深圳

指导单位：



主办单位：



时间：2021年5月21日-22日

# 智能运维的实用性和易用性探索

## 智能运维中的数据管理和平台应用

王鹏 复旦大学



# 王鹏

复旦大学，教授，计算机科学技术学院

在数据库和数据挖掘领域顶级会议和期刊SIGMOD、VLDB、ICDE、IEEE TKDE、ICDM上发表论文30多篇，主持和参与科技部重点研发专项、国家青年973、自然科学基金重点、面上基金、上海市科委/经信委的多个项目，以及华为、微软、IBM、EMC、爱立信等企业的资助项目

# 目录

CONTENTS

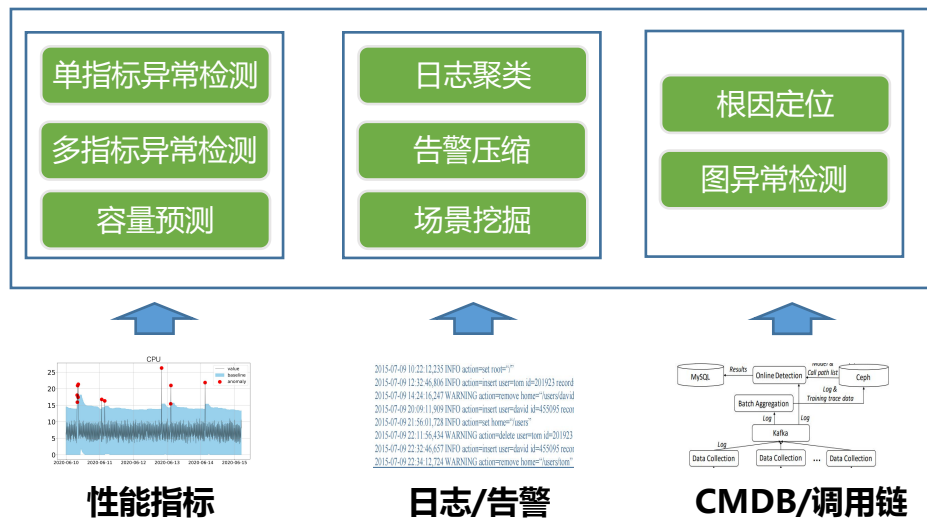
- 1 背景
- 2 数据语义融合
- 3 数据管理查询
- 4 总结

# 背景

01

# 研究现状

- 数据类型日益丰富
  - 时间序列（性能指标）
  - 离散事件序列（日志/告警）
  - 图数据（CMDB、调用链）
- 算法效果不断提升
  - 单源数据算法
  - 多源数据算法



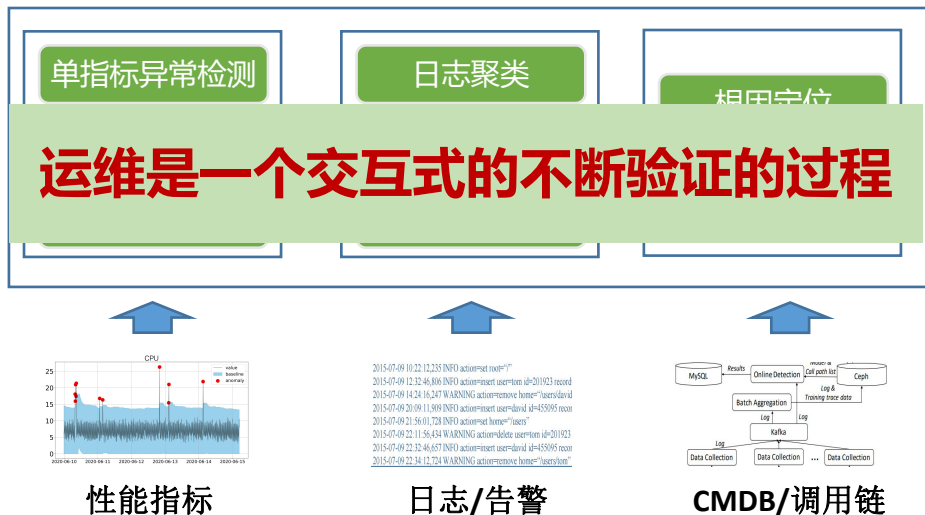
# 仅有算法是不够的

## • 算法研究阶段

- 算法发现告警A和B经常一起出现，需要回答“这是偶然现象吗”
- **Common Sense, 例外, 有价值?**

## • 算法应用阶段

- 算法发现告警C是根因，需要回答“这个故障之前出现过吗”
- 数据库告警模板发生时，希望查看对应时间段的CPU和内存波动情况
- **历史、多源数据的参考极为重要**



# 智能运维能力

## 算法能力

- 异常检测算法
- 日志聚类算法
- 根因定位算法

## 数据语义融合能力

- 多源数据中的实体匹配
- 实体关联
- 多源数据的特征关联



## 异构数据管理能力

- 大规模时间序列数据、日志/告警文本数据、图数据、结构化数据的统一管理

## 数据探索能力

- 异构数据的统一查询
- 语义查询



针对时序数据、文本数据、图数据、结构化数据

- 1.实现统一的数据管理
- 2.在语义层面进行融合
- 3.实现跨数据源的查询



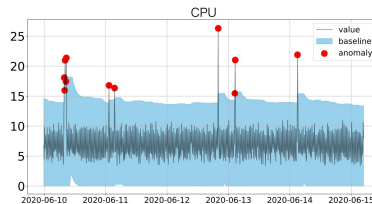
- **运维数据的充分利用**
- **为运维人员排障提供便利**

# 数据语义融合

02

# 动机

- 从语义层面将数据进行有效融合
  - **运维数据都是对IT系统的某个对象的描述**
- 支持告警/日志和性能指标的关联
- 支持基于自然语言的查询引擎

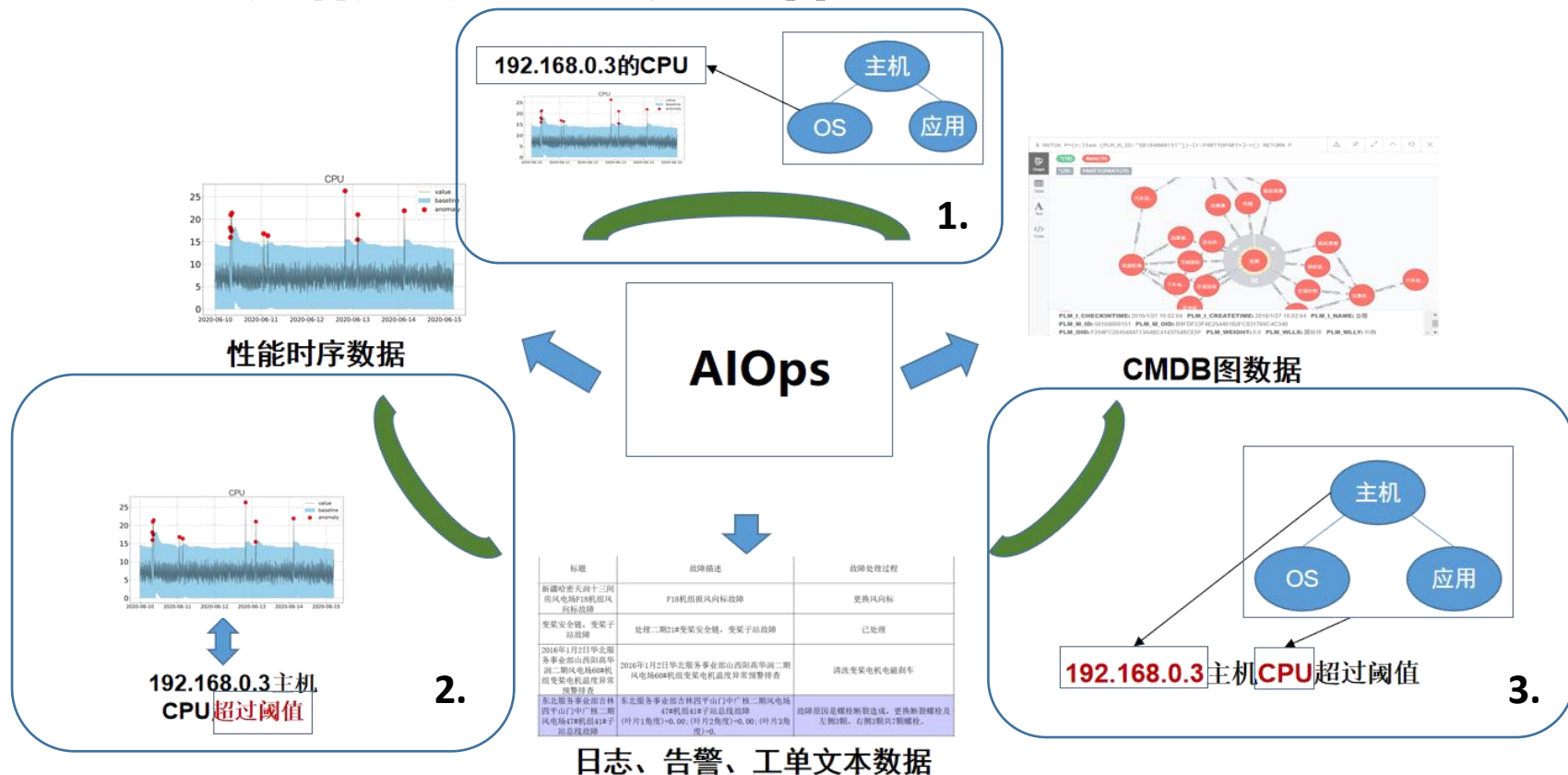


性能指标

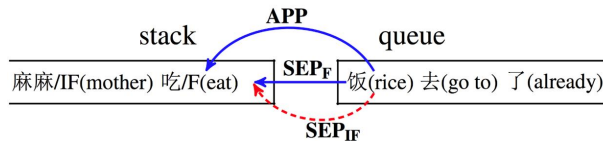
服务器host01: total cpu is now  
95.10%, 高于阈值 (90%)

告警

# 运维数据关联和知识图谱



# 步骤一：实体提取



• 输入文本：处理二期21#变桨安全链，变桨子站故障...

• 用户词库：处

1. 分割：处理

2. 更新用户词库：处理，二期，故障，21#变桨安全链，变桨子站

• 迭代1、2步

**运维数据都是对IT系统的某个对象的描述**



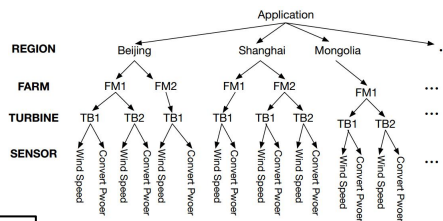
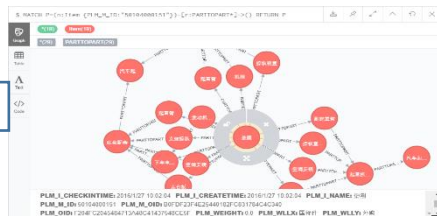
从自然语言中  
提取实体

提取、关联告警  
中的非正式描述  
实体

从更大范围  
提取实体

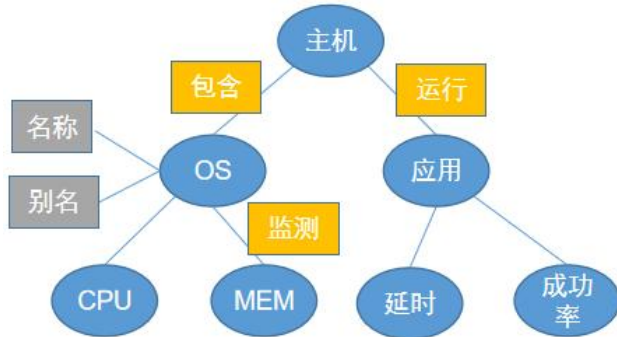
# 步骤二：实体图和时序元数据融合

扩充后的实体图



时序元数据

基于时序结构化元数据进行匹配

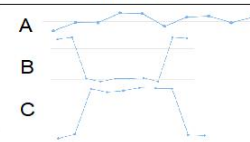


最终结果

- 将监测时序数据id添加到实体图
- 实现CMDB数据和时序数据的融合

# 步骤三：文本特征和时序特征的融合

- 基于**弱标签分类算法**，学习故障描述文本对应的时序模式
- 在图谱中添加相应的时间序列模式
- 基于**时间序列近似匹配算法**，在历史数据中找出更多实例

语义模式库			
故障名称	文本特征	时序特征	时序模式库
风机发电机功率故障	风速较大，功率较小。	时序模式A 时序模式B	
...	...	...	

- Jiaye Wu, Peng Wang, Ningting Pan, Chen Wang, Wei Wang, Jianmin Wang, KV-match: A Subsequence Matching Approach Supporting Normalization and Time Warping, ICDE 2019
- Zicheng Fang, Peng Wang, Wei Wang, Efficient Learning Interpretable Shapelets for Accurate Time Series Classification. ICDE 2018
- Hanbo Zhang, Yawen Wang, Peng Wang, Wei Wang, Burst-based Event Classification on Weakly Labeled Time Series Data of Sensors, IEEE 6th International Congress on Big Data, 2017

# 用途

- 基于自然语言的时间序列查询
  - 性能指标数据覆盖面更广，告警/日志数据易用性更好
- 告警数据的合理性验证
- 融合告警数据、CMDB、性能指标数据的根因定位



# 数据管理和查询

03

# 查询工具集

✓ ① 面向自然语言的运维数据查询

✓ ② 拖拽式数据处理引擎

✓ ③ 面向时间关联的数据查询

④ 面向异常检测的数据查询和可视化

⑤ 异构数据查询引擎



提升查询的易用性



提升运维数据的查询表达能力



提升异构数据查询能力

# 1 基于自然语言的运维数据查询

- 提升运维过程中运维人员的数据探索能力
- 核心功能
  - 运维数据的统一管理
  - 自然语言到SQL的转化引擎

表1-1 数据库自然语言查询系统及关键步骤技术

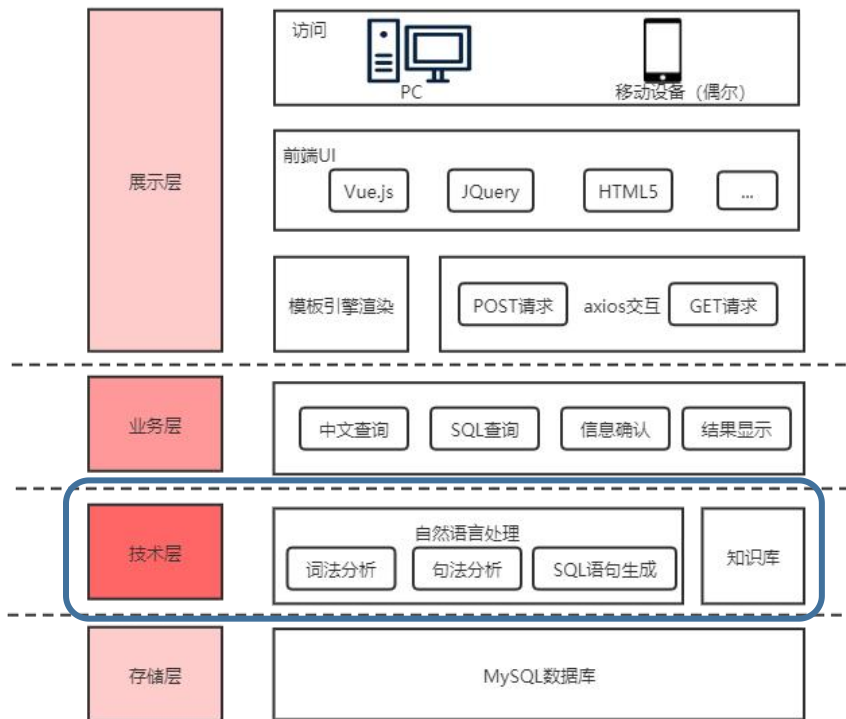
系统	预处理	词法分析	句法分析	SQL 语句生成
NaLIR <sup>[10]</sup>	Stanford Parser <sup>[11]</sup>	WordNet <sup>[12]</sup> + 用户交互	候选路径选取 + 用户交互	启发式查询树 + 用户交互
SQLizer <sup>[13]</sup>	Sempre <sup>[14]</sup>	word2vec <sup>[15]</sup>	手写规则	手写规则
Seq2SQL <sup>[16]</sup>	Tokenizer + Stanford CoreNLP <sup>[17]</sup>	GloVe <sup>[18]</sup> + character n-grams <sup>[19]</sup>	——	——
SQLNet <sup>[20]</sup>	Tokenizer + Stanford CoreNLP <sup>[17]</sup>	GloVe <sup>[18]</sup>	——	——



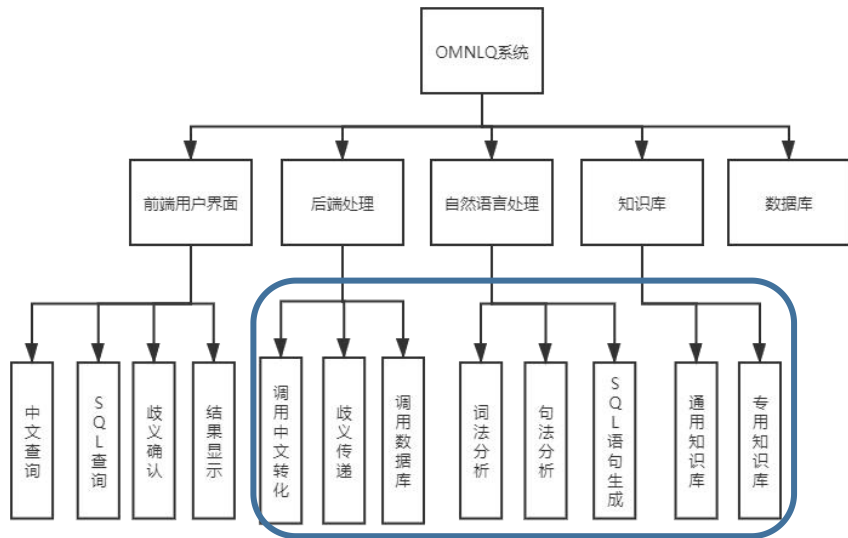
1. 找发生告警次数最多的主机名为Server1的告警类型。
2. 发生毛刺异常次数最多的应用。
3. CPU占用率最高的应用。
4. 近15分钟全部交易指标异常。
5. 每天的交易失败次数。
6. 过去7天同一时刻应用名为app1交易量情况。
7. 最近10分钟内应用名为app1的交易异常分布。
8. 最近8小时内每分钟的平均响应时间。
9. 最近9分钟突增或突降的指标有哪些？

# 基于自然语言的运维数据查询

## 系统架构



## 核心模块



# 运维知识图谱

## (1) 实体词典

(“异常”, “outlier”)  
(“主机”, “server”)

## (2) 属性词典

(“大于”, “>”)  
(“等于”, “=”)

## (3) 属性值词典

(“业务型”, “指标分组”)  
(“突增”, “类型”)

## (4) 修饰词词典

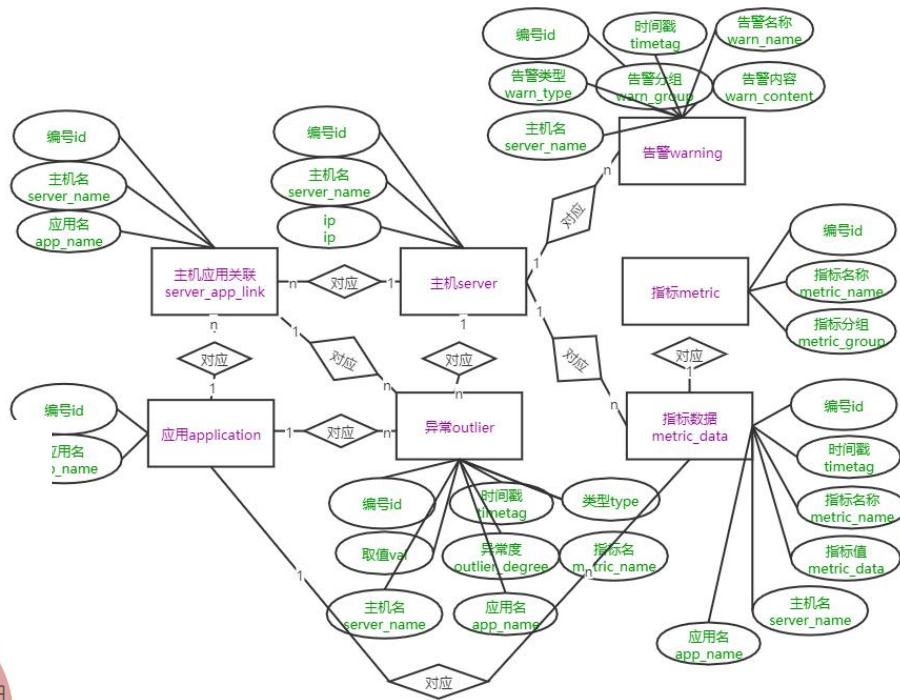
(“ outlier ”, [‘id’,  
‘timetag’, ‘val’, ‘outlier\_degree’,  
‘type’, ‘metric\_name’,  
‘server\_name’, ‘app\_name’])

## (5) 专用分词词典

“交易量”、“时间戳”

## (6) 近义词词典

(“机器”, “服务器”) -  
> “主机” (“server”)



## (1) 聚集词词典

(“计数”，“COUNT”)  
(“最小”，“MIN”)

## (2) 比较关系词典

(“大于”，“>”)  
(“等于”，“=”)

## (5) 通用分词词典

“小于等于”

## (3) 固定搭配词典

(“分组”，“GROUP BY col”)  
(“排序”，“ORDER BY col”)

## (4) 逻辑关系词典

(“与”，“AND”)  
(“或”，“OR”)

“突增或突降”：

outlier.type='突增' OR  
outlier.type='突降'

# 查询处理引擎

## 1. 词法解析

- 分词
- 数据库语义标注
- 语义消歧

“最近1天内存异常程度超过80%的异常分布”



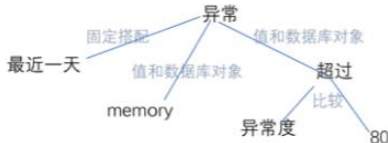
[‘最近 1 天’/固定搭配,  
‘memory’/属性值/所属属性  
‘metric\_name’/所属实体‘metric’/有歧义/歧义列表  
[‘metric’, ‘metric\_data’, ‘outlier’],  
‘异常度’/所属属性‘outlier\_degree’/所属实体‘outlier’,  
‘超过’/操作符‘>’,  
‘80’,  
‘的’,  
‘异常’/所属实体‘outlier’, ‘分布’]

```
SELECT `outlier`.`id`, `outlier`.`timetag`, `outlier`.`val`,  
`outlier`.`outlier_degree`, `outlier`.`type`, `outlier`.`metric_name`,  
`outlier`.`server_name`, `outlier`.`app_name`  
FROM `outlier`  
WHERE timetag >= DATE_SUB(CURDATE(), INTERVAL 1 DAY)  
AND `outlier`.`metric_name`='memory'  
AND `outlier`.`outlier_degree` > 80
```



## 2. 语法解析

- 语义依存树
- 句法分析



```
{object=outlier.allattribute},  
{condition=[ timetag >=DATE_SUB(CURDATE(),INTERVAL 1  
DAY), `outlier`.`metric_name`='memory', `outlier`.`outlier_d  
egree` > 80 ]},  
{table=outlier}
```

## 3. SQL生成

# 系统界面

请输入中文查询:  点击确定

请检查英文查询:  点击确定

请确认
 
点击确定 ?

暂无数据

共 0 条 < 1 > 请选择

当前表: 异常outlier

异常.编号	异常.时间戳	异常.取值	异常.异常度	异常.类型	异常.指标名称	异常.主机名	异常.应用名
33	2020-03-26 02:57:39	91.55	0.32	突降	cpu占用率	server1	app66
57	2020-03-13 00:53:48	29.05	0.7	突降	交易量	server1	app66
283	2020-03-11 05:48:37	0.8	0.53	突降	磁盘访问量	server1	app66
931	2020-03-16 23:57:00	51.54	0.47	突增	应用访问量	server1	app66
1156	2020-03-28 10:48:45	57.23	0.85	周期	磁盘访问量	server1	app66
1236	2020-03-01 20:38:59	64.66	0.65	周期	cpu占用率	server1	app66
1308	2020-03-29 04:44:04	64.1	0.61	周期	memory	server1	app66

共 25 条 < 1 2 3 4 > 请选择

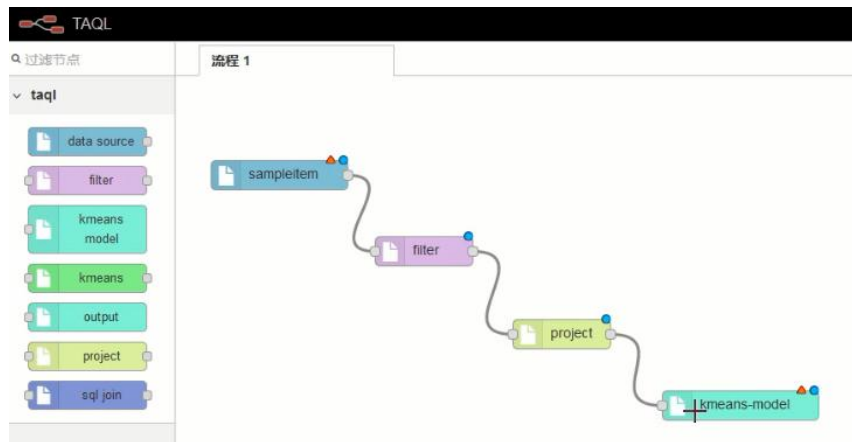
## 查询示例

1. 找发生告警次数最多的主机名为Server1的告警类型。
2. 发生毛刺异常次数最多的应用。
3. CPU占用率最高的应用。
4. 近15分钟全部交易指标异常。
5. 每天的交易失败次数。
6. 过去7天同一时刻应用名为app1交易量情况。
7. 最近10分钟内应用名为app1的交易异常分布。
8. 最近8小时内每分钟的平均响应时间。
9. 最近9分钟突增或突降的指标有哪些？



## ② 拖拽式运维数据分析引擎

- 便于领域专家结合不同分析算法  
搭建分析流程
- 融合了异常检测、聚类、场景挖掘等多种算法
- 支持不同语言开发的算法
- 支持输入数据格式的智能学习



# 主要算法

## ■ 时间序列数据挖掘

- 时间序列分类, sax-vsm, fast-shapelet
- 时间序列弱分类: matrix-profile based
- 聚类: k-shape
- 状态切分: Autoplait, pHMM, mp-based supervised
- 频繁子序列挖掘: motif
- 异常检测: STL, ripple, SOM
- 相关性分析: tslrm, Jocor
- 序列匹配: DSTree
- 子序列匹配: , ucr-ed/dtw, kv-match, onex

## ■ 日志/告警分析

- 模板提取: Drain、Spell
- 场景挖掘: Fp-growth、community-based
- 根因定位: mutual information
- 正则表达式处理
- 变量提取

### 3 面向时间关联的数据查询

Log Type	Log Content
$E_1$	2019/8/6 15:00 Adding a new node: /default-rack/192.168.0.231:50010
$E_1$	2019/8/6 15:01 Adding a new node: /default-rack/192.168.0.232:50010
$E_2$	2019/8/6 15:02 Adding new storage ID DS-efe44b9ea549 for DN 192.168.0.231:50010
$E_2$	2019/8/6 15:02 Adding new storage ID DS-efe54b9sa352 for DN 192.168.0.232:50010
$E_3$	2019/8/6 15:03 Number of failed storage changes from 0 to 0
$E_4$	2019/8/6 15:04 BLOCK* fsync: /hbase/WALs/hadoop5
$E_5$	2019/8/6 15:05 BLOCK* registerDatanode: from DatanodeRegistration(192.168.0.231:50010)

```

SELECT A.*, B.*, C.*
FROM (SELECT * FROM HDFS WHERE LogType =  $E_1$ ) A
INNER JOIN (SELECT * FROM HDFS WHERE LogType =  $E_2$ ) B
ON 0 <= TIMESTAMPDIFF(MINUTE,A.Timestamp, B.Timestamp) <= 5
AND A.IP = B.IP
INNER JOIN (SELECT * FROM HDFS WHERE LogType =  $E_5$ ) C
ON 0 <= TIMESTAMPDIFF(MINUTE,A.Timestamp, C.Timestamp) <= 5
AND 0 <= TIMESTAMPDIFF(MINUTE,B.Timestamp, C.Timestamp) <= 5
AND A.IP = C.IP

```

SQL查询

```

PATTERN ( $E_1, E_2, E_5$ ) WITHIN 5 minute
BETWEEN 2016/08/06 15:00 AND 2016/08/06 15:10
AND  $E_1.IP = E_2.IP$ 
AND  $E_1.IP = E_5.IP$ 

```

PLQ查询

**在告警序列中，告警间通常具有关联关系，这些告警均由同一系统行为引发  
这些告警的集合称为场景**

shared memory realm does not exist

ORACLE not available

could not obtain authorized session

**场景1**

链路异常

射频业务异常

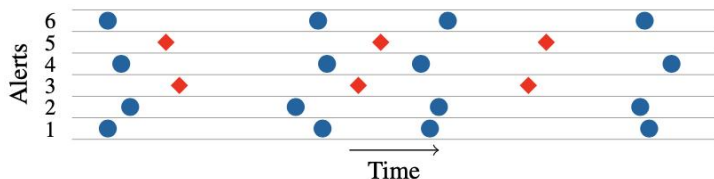
小区不可用异常

**场景2**

在告警序列中，告警间通常具有关联关系，这些告警均由同一系统行为引发  
这些告警的集合称为场景

## 行为信息

告警出现规律中蕴含的行为信息



FP-Growth  
Apriori  
SWIFT, ...

## 语义信息

告警文本中蕴含的语义信息

Content
Memory utilization (90.3%) exceeds configured threshold (90.00%)
Memory util reached threshold 99%

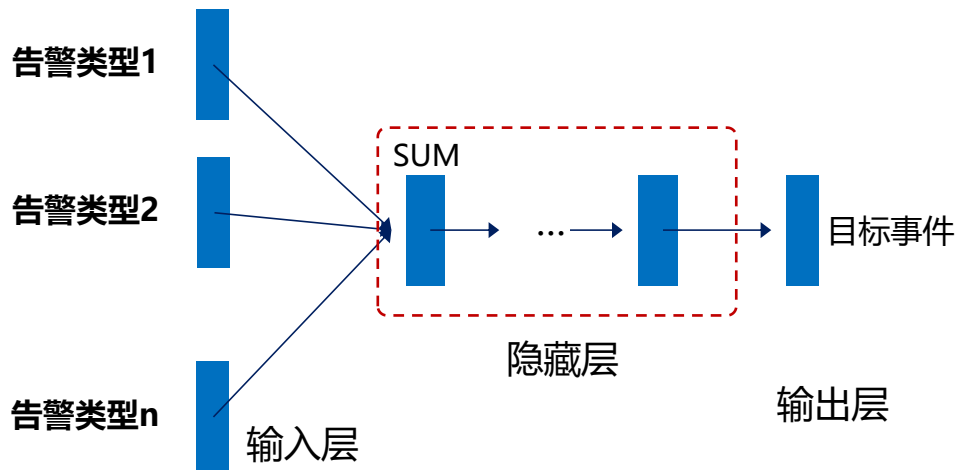
Bag of Words,  
Jaccard,  
Word Embedding, ...

目标：融合行为信息和语义信息，基于深度学习模型进行场景挖掘

# 利用行为信息

行为序列：告警在过去24小时每一分钟发生的次数

利用深度学习模型(Continuous Bag Of Words), 学习关联告警间相同的行为特征

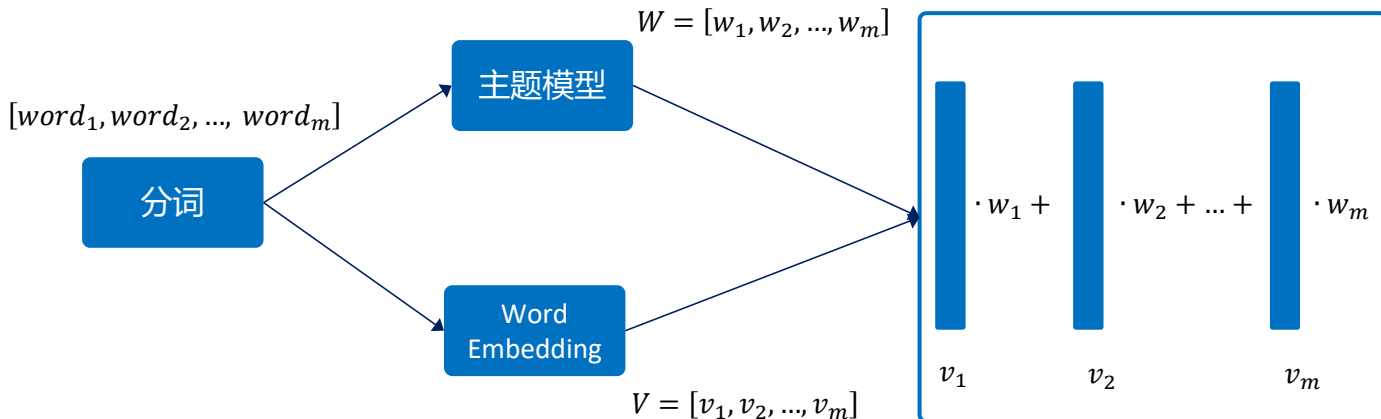


类CBOW模型

# 利用语义信息

告警内容包含多个单词，每个单词对关键语义的贡献程度不同

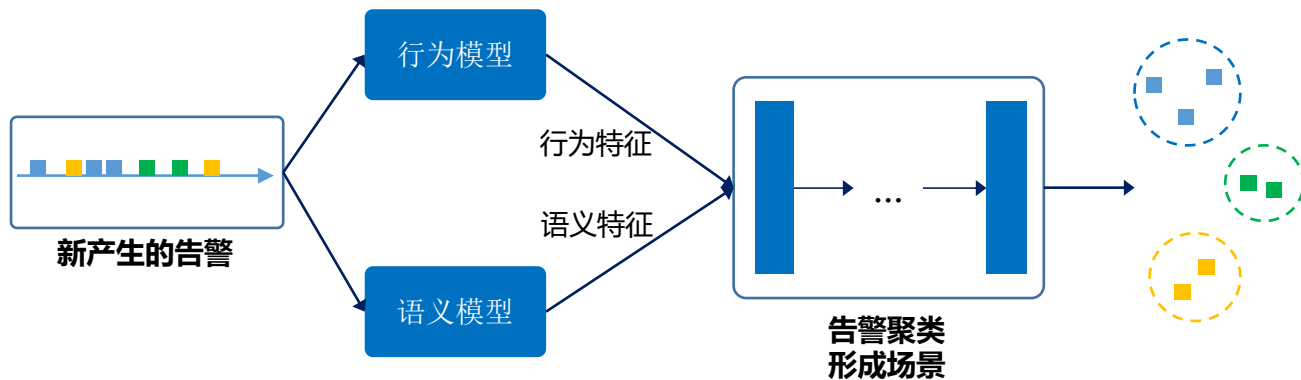
示例告警 The **TIME\_WAIT tcp connection** number is 3018 is **great** than **threshold** value 3000 please pay attention..



将单词在告警所属主题内出现的概率作为对事件语义的贡献程度

## 场景挖掘

整合告警的行为信息和语义信息，结合深度学习模型在线地对告警进行聚类

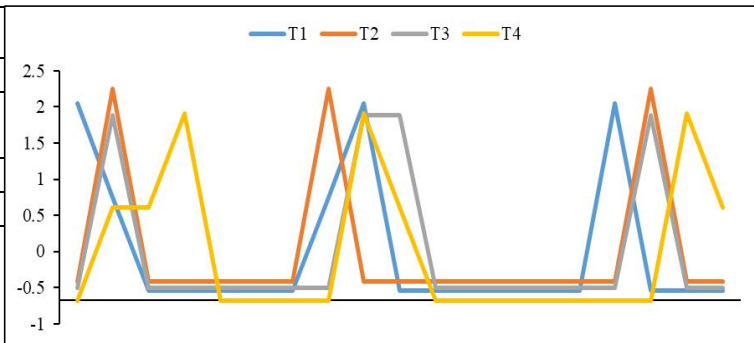




# 结果示例

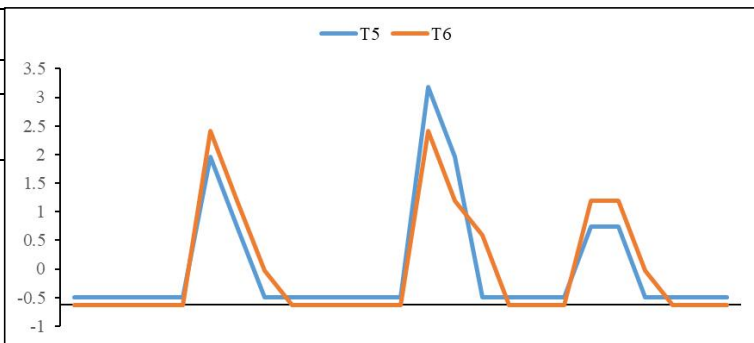
## 告警

Timestamp	Type	Content
2021/5/2 14:18	T1	Memory utilization (90.3%) exceeds configured threshold (90.00%)
2021/5/2 14:19	T2	instance XXX database XXDB tablespace XXTable utilization 75 exceed threshold 70.00
2021/5/2 14:19	T3	Memory util reached threshold 99%
2021/5/2 14:20	T4	CPU Util reach 90.2%, exceeds threshold 90.00%



## 日志

Timestamp	Type	Content
2020/10/23 1:21	T5	check pass; user unknown
2020/10/23 1:21	T6	authentication failure; logname= XXX uid=0 euid=0 tty=XXX ruser= XXX rhost= XXX



# 面向时间关联的数据查询

- 典型应用

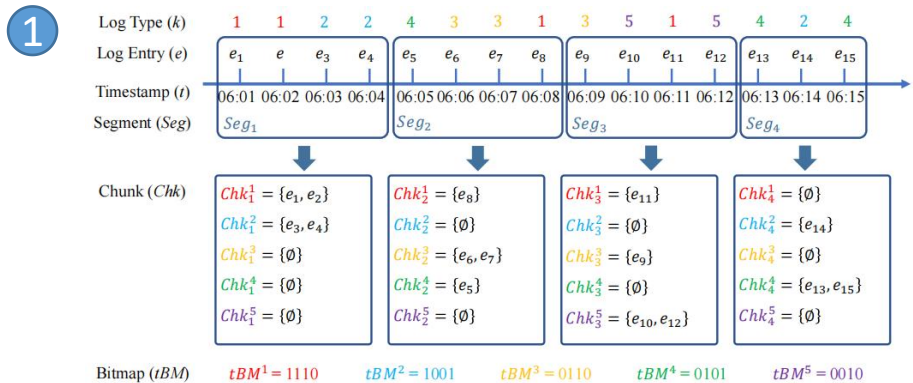
- 告警数据中的场景分析
- KPI数据和日志/告警数据的关联分析

```
PATTERN ( $E_1, E_2, E_5$ ) WITHIN 5 minute  
BETWEEN 2016/08/06 15:00 AND 2016/08/06 15:10  
AND  $E_1.IP = E_2.IP$   
AND  $E_1.IP = E_5.IP$ 
```

面向时间关联的数据查询

**时间关联是运维分析的核心目标，  
也是关联多源数据的重要手段**

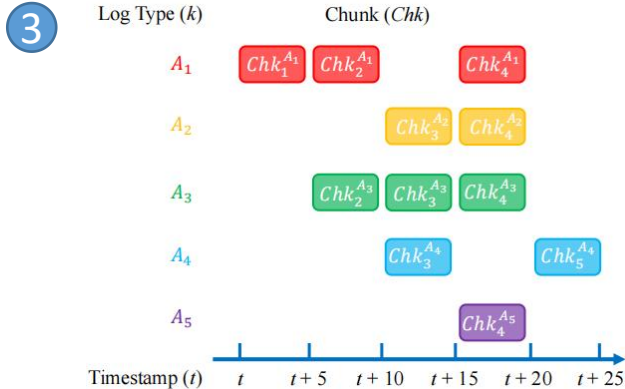
# 面向时间关联的数据查询



## 基于bitmap的数据分块

2

AND、OR、L-SHIFT、R-SHIFT、FILL、M-AND  
自定义bitmap操作集合

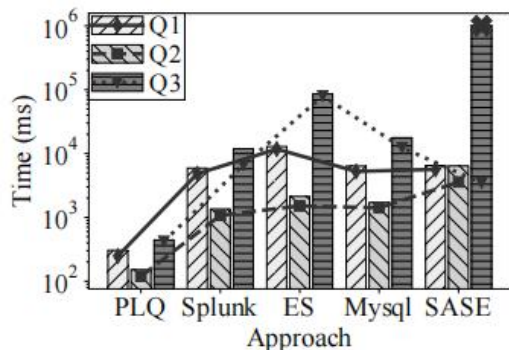


$$BM^{A_i} = BM_P^{A_i} \& BM_T^{A_i} \& BM_S^{A_i} \& BM_V^{A_i}.$$

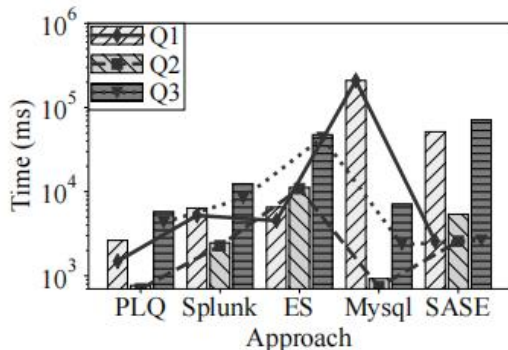
## 基于bitmap的查询处理

# 面向时间关联的数据查询

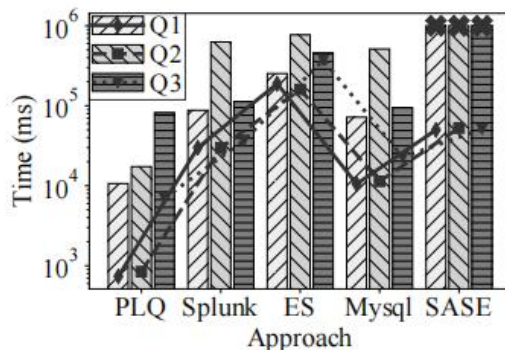
HealthAPP



OpenStack



HDFS



**可扩展作为性能指标、日志、调用链数据的统一查询工具**

**例如：某类型的指标异常和某种特点日志是否总是一起发生**

# 总结

- 在算法设计、测试和应用过程中，数据探索查询起到重要的作用
- 多源异构数据需要从语义层面进行有效融合
- 查询引擎应面向运维数据特点且具有高易用性



# Thanks

高效运维社区  
开放运维联盟

荣誉出品