



CONTENT

- 数据安全治理的主要任务
- ·数据安全治理若干关键技术
  - 总结与展望



# 大数据是一场技术革命,一场经济变革,也是一场国家治理的变革



"数据已成为国家重要的基础性战略资源"

2015年 8月

国务院印发《促进大数据发展行动纲要》

首次提出"国家大数据战略"

2015年 10月

中共十八届五中全会

推动政务信息系统互联和公共数据共享

2016年 9月

国务院印发 《政务信息资源共享管理暂行办法》 对十三五时期大数据产业发展进行整 体规划、全面部署

> 2016年 12月

工信部印发 《大数据产业发展规划2016-2020年》 推动实施国家大数据战略

2017年 12月

习近平总书记在中央政治局第二次 集体学习上的讲话

# 大数据时代,数据安全尤为重要



### 数据安全关系到国家安全

例: 2017年哈罗德·托马斯·马丁三世窃取美国政府信息系统中超过50TB数据,包括至少5亿页政府机密文件



## 数据泄露日趋严重

71%的数据泄露以金钱为目的, 25%涉及战略目的的间谍活动; 69%的网络攻击来自外部人员, 34%涉及内部人员的窃取

### ■数据安全法规和标准逐渐完善

2017: 《网络安全法》实施;

2019: 《等保2.0》实施;

2020: 《密码法》实施;

2020: 《数据安全法》《个人信息保护法》

征求意见

### ■数据安全需要有系统化思维和建设框架

我国大数据安全建设仍存在安全防护有技术、少体系,安全监管缺手段、少抓手,数据管理有规划、缺落实等问题,数据安全治理将数据安全技术与数据安全管理融合,对于提升数据安全,促进数据共享利用具有重要意义

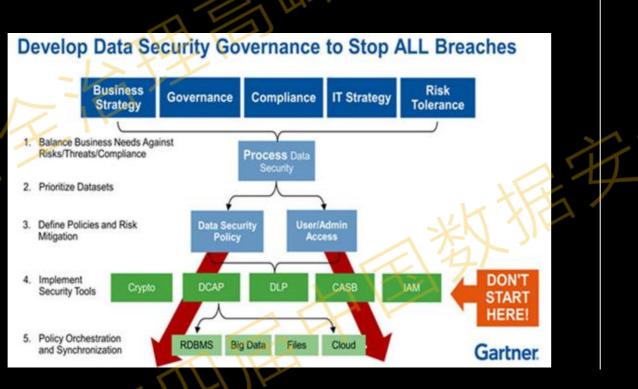


# 什么是数据安全治理?



## Gartner数据安全治理理念

数据安全治理不仅是一套用工具组合的产品级解决方案,而是从决策层到技术层,从管理制度到工具支撑,自上而下贯穿整个组织架构的完整链条。



## ■微软的DGPC理念

隐私、保密和合规性框架的数据治理计划,围绕人员、流程和技术三个核心能力领域组织。基于信息生命周期,从安全基础架构、身份和访问控制、信息保护、审计和报告四个技术领域提供保证,并遵循数据隐私和保密原则。

## 中国网信联盟数据安全治理委员会

"让数据使用更安全"为目的的安全体系构建的方法论。

《数据安全治理白皮2.0》

### 愿景: 让数据使用更安全

求覆盖

分

新级对象 角色授权 担织构建 资产梳理 衰略制定 过程控制 亍为稽核

安全框架 细细 等較知

人员组织 策略规范

# 数据安全治理技术体系

数据采集安全

是全技术



## 数据生命周期安全过程域

### 数据生存周期安全过程均

●PA20数据安全策略规划

通用安全过程域

●PA22合规管理

### 数据处理安全

- ●PA14数据导入导出安全
- ●PA13数据
- ●PA12数据正当使用 ●PA11 数据分析安全
- ●PA10数据

●PA23数据资产管理

### 数据交换安全

- ●PA16数据发布5
- ●PA15数
  - ●PA17 娄

●PA24数据供应链安全

●PA25元数据管理

●PA30安全事件应急

- ●PA19存储媒体销毁处置
- ●PA18数据销毁处置

数据分级分类

合规 漏洞 配置 权限

## ·数据安全治理技术支撑体系

业务访问安全

运维访问安全

测试开发安全

数据外发安全



#### 数据安全治理技术支撑体系

#### 安全状况摸底

#### 数据资产梳理与定位

数据库安全风险扫描

### 行为审计与分析

权限变化监控

异常行为分

建立安全基组

#### DATA SECURITY GOVERNANCE

# 数据共享的主要问题

利用大数据打造企业核心竞争力,提升政府治理能力和公众服务水平,已成为社会的 共识。数据是智慧社会的支撑,及时开放、共享数据,充分挖掘数据资源"宝矿",才 能发挥最大效益。

国际上"开放政府联盟"宣布成立,八国集团首脑签署了《开放数据宪章》。在此期 间,美国、英国、法国、加拿大和澳大利亚等西方发达国家和巴西、阿根廷等新兴国 家纷纷推出数据开放的国家战略。

2015年国务院印发的《促进大数据发展行动纲要》中首次提出"大力推动政府部门数 据共享"以来,各级政府部门以及医疗、交通等重点行业积极响应。尽管如此,大数 据共享的发展仍然不容乐观。

### 用户担心个人隐私暴露,不愿意共享数据

隐私 原因







政府、企业等实体担心数据共享引发敏感信息泄露,违反法律、法规



《欧盟通用数据保护条例》









孤立的数据难以形成合力, ,阻碍数据资源的充分利用

#### 1、定义

- ➤属性加密方案(Attribute Based Encryption,ABE)是一种新型公钥加密技术,能够在加密的同时 实现对数据的细粒度访问控制。
- > 不再需要部署集中式的访问控制网关,是未来实现密态数据共享的重要工具之一。

#### 传统解决方案



#### 专统解决方案的不足:

- **—**₹₫—
- 访问控制网关容易成为重点攻击目标
- · 密钥管理复杂
- 很难实现细粒度的访问控制
- 访问控制策略不够灵活

#### 属性加密方案



#### 《性密码的优势:

- 1名
- 在加密的同时实现访问控制,不再需要访问控制网关
- ▶ 家钼管理简单
- 2现细粒度的访问控制,可精确到文件
- 灵活访问控制策略,支持与、或、优先级



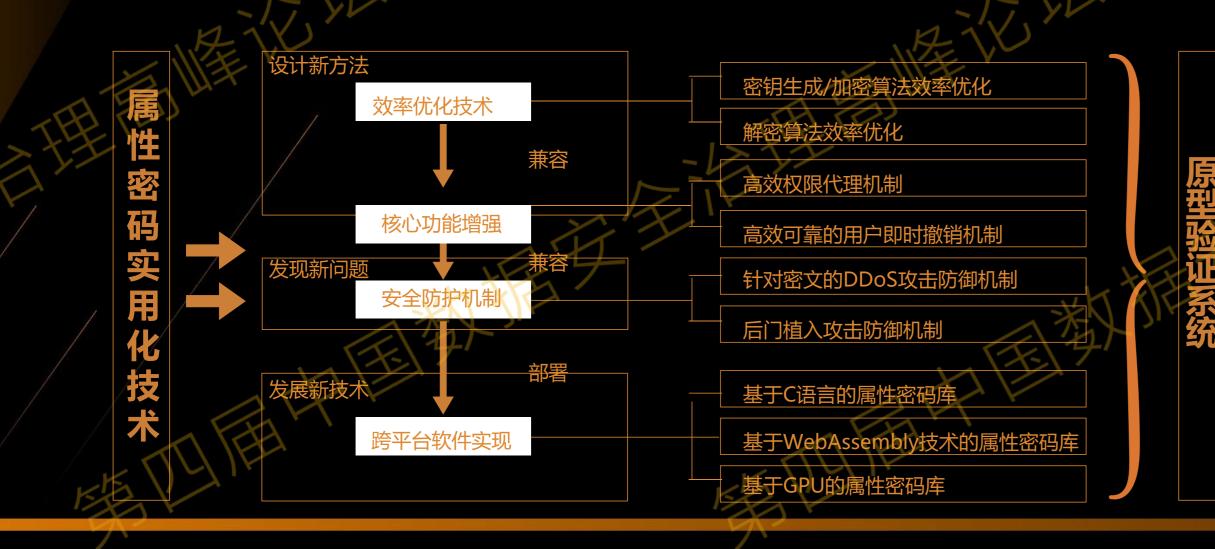
### 2、应用场景——密态数据的访问控制

- ➢同时提供加密和细粒度访问控制功能
- >访问控制策略由传统集中式设置变为分布式设置,适用于分布式场景
- >适配结构化数据(如数据库页表)、非结构化数据(如文档、图片等)

### 3、国内外技术进展

- ➤从2005年至今,属性密码备受学术界和工业界关注,一直是热门研究方向。
- ➢国内外研究侧重纯理论、特定场景解决方案研究,研究成果之间不成体系。
- >目前属性加密实用化研究较为分散,互不兼容,距离实用化还有一定距离!





应用落地解决方案等领域形成一系列创新研究成果:

围绕属性加密方案的实用化技术,中科院信工所团队在效率优化技术、核心功能增强、安全防护机制、跨平台软件实现、

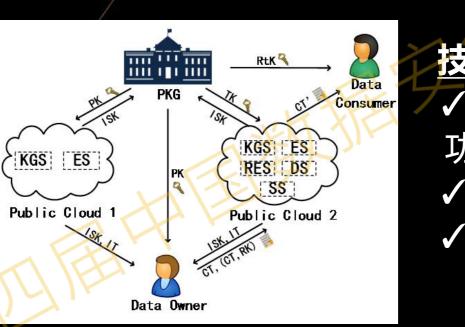
- ➤在IEEE TDSC、IEEE TIFS、IEEE TPDS、IEEE TM、IEEE TSC、ESORICS等期刊和会议上发表学术论文20余篇。
- >形成跨平台软件函数库,可兼容主流操作系统和开发环境。

DATA SECURITY GOVERNANCE

# S Community

### • 支持快速权限代理的加密数据共享方案

**主要问题**:属性加密方案的核心算法和权限代理的模指数、双线性对运算次数与属性个数呈正线性相关。例如,一次加密操作可达403次模指数运算

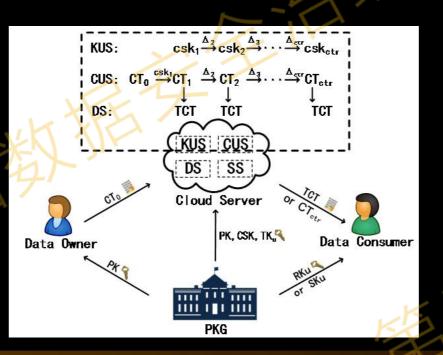


#### 术创新:

- ✓ 提出了基于外包计算的支持快速权限代理的属性加密方案,成功将所有核心算法和权限代理算法的在线计算量从O(n)到0
- ✓ 解决了基于属性加密的密态数据共享技术的效率瓶颈
- ✓ 该成果发表在CCF网络与信息安全领期刊IEEE TDSC

### ・支持用户即时撤销机制的属性加密方案

**主要问题**:实际部署的密码系统离不开用户撤销和用户密钥撤销机制**既存的属性密码撤销机制无法兼容效率和可靠性** 

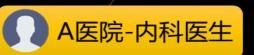


### 技术创新:

- ✓提出了基于分步解密思想的可撤销属性加密方案,可立即对用户完成撤销操作,同时抵抗撤销密钥泄漏攻击
- ✔解决了现有属性加密撤销机制无法兼容效率和可靠性的问题,解决 实际部署的后顾之忧
- ✓ 该成果发表在期刊IEEE TSC















权限不符合

✓ 支持端到端加密,确保数据中心无法获得明文数据, 打通共享通道

### 数据库字段级加密和访问控制

														-200
	页表存	诸——全部	郭加密	Edit: 🚄	Export/Impo	ort: 🖫 🖔	1							
	id	name	address		type	phone	contact	power_type	last_mete meter	_num delta_num	unit_price	total_price		
	2234f25d00	a8d717d3e32bba6b	c95acd801219305	e4b2deb6d	a6205574d0da1055	ec7b2eefd574bcb7	7d 40270f7d2acc35ba24ca29	5b094e388953f717b4	ef56e4e9 258d6	5853 066e3ded	29dac9b8d2b3f64	dcacde19dc14511d3d0e9159ce7d8c1		
	6e37f10bb0	7248abb2dc85752fa	67c1a144fa895c29	9d18cb410e	8a0b7bad45767244	ca2fb5e45914de75	0 c1f8d943417ba7a194b3b.	109fe04e81107dcf7e3	6b87edcd 422a6	51cd b21b480f	a547b39503b3f84	496183fd1bc49e0bffd899b0d087e8f9	1	S
	54daccab0c	09e2ef21de4c5f7b4	3b138790d9687f52	2a07063d8	1f246f03970851fa42	cbd9c078e9de2cb9	f1 af51d51a197b0d0d311d0	ecb853572ecf3b1cdc2	. cdebd937f bd959	e4e7 c145b5b6	356960bf787f6e20	15b049d75c5e83fdf367169b6555e60	4	<b>⊩</b> 1
	a8ab9b5c73	e72ba7d3b6f4ef409	cd131b0a36b57da	5390e9fdd	bd79fb3bc0fd1fc193	b27158d621be685	dd 5e56dc0a2d45b4163b764.	248ae3403c4f4b57a4	f53e6272f 09750	b485 9eb261ec	4c6dc7e9957b4a6	3141ef6e2deebac98ceb8b58f683b6d	d	2
	4fbb204e3e	51491a0863cd4686	70a0afe554de1ac6	6ad26599bc	67a919ab94d57fe8b	1d480f19a662f7cde	e4 8ca596ce6759f169146ac1	5d1c8870730203b5c4	1834cb3d 9ac69	3a40 893e894d	9c0ed82382f499a	d989f58b261cba582c7e8d52ca30cba		3
	0419101072	0e8ed5c88639aff9a	384d0b0d9b81857	96cb63594	2828967e3228adf4d	e11fd68668c18cf47	c 27b8b2a594dc109ce2278.	1a7b1eba05123f5fb4a	. 972136ec 0b8c4	005c dd9544bf	46721c8f06d2563	44190d0dc4008a1f5408b152cea7c10	) a	4
	0b4b903233	7989d6a3115c8852a	. e28e744e0b3f0406	6898c4008f	0a85a00c8b4823af1	017a3f605b6f7456	df 804052a670f23bbed0532.	ff0529ecfa1764043663	. c7085704 f58746	e0ed 2af9e31d	ab3c91f8b284a0a	81b24a5d596bc2dd952a49e398eb64	d	5
	6511bbe0c3	3858d8dd50a6caecf	eb5aece919ece25	1a9d2908b	7f4383242a6d9ea3d	7a828037e86799b	d3 0d02eb5e2b11395fc75b3c	e05482ba1ca6ab9ce4	1351fea1 ab8c6	c370 1754df7e	2092b372a85ec2e	74c5f5b4ea130b6bbda8eb943e3c3d1		6
	0f57c48b9a	ec9f0e2f21e552e84	403db1a56d0bd7fe	ee383f4138	d4493ba88b7e2e4d	88db280bd138788	53 881b77de3567de9da07eb.	7557a149b848838e7d	. b4a83591 b4a5b	2552 d5b03d57	6bed286e3ff9309b	f347e1a3cf3089361295a5f5f9e54f17c	3	7
Ī														8

- ✓数据库表的所有字段均使用ABE加密。
- ✓ 不同用户使用各自密钥解密同一张页 表,得到不同的字段。

								1 - 1	•			
	<u> </u>	<b>凌员页面</b>	Edit: 🔏	Export/Impo	ort: 📳 🐻						20	
seq	id	name	address	type	phone	contact	power_type	last_mete	meter_num	delta_num	unit_price	total_price
1	800102002	a8d717d3e32bba6b	科学城尖塔山路2号	a6205574d0da1055	ec7b2eefd574bcb77d	. 40270f7d2acc35ba24ca29	5b094e388953f717b4	9921006	9926867	5861	29dac9b8d2b3f64	dcacde19dc14511d3d0e9159ce7d8c
2	800102003	7248abb2dc85752fa	广东省广州市黄埔区科学城科	8a0b7bad45767244	ca2fb5e45914de750	c1f8d943417ba7a194b3b	109fe04e81107dcf7e3	1121621	1128432	6811	a547b39503b3f84	496183fd1bc49e0bffd899b0d087e8f9
3	800102004	09e2ef21de4c5f7b4	广东省广州市黄埔区科学大道	1f246f03970851fa42	cbd9c078e9de2cb9f1	af51d51a197b0d0d311d0	ecb853572ecf3b1cdc2	22651710	22655502	3792	356960bf787f6e20	15b049d75c5e83fdf367169b6555e60
4	800102005	e72ba7d3b6f4ef409	广东省广州市先烈中路1号	bd79fb3bc0fd1fc193	b27158d621be685dd	5e56dc0a2d45b4163b764	248ae3403c4f4b57a4	17615139	17623592	8453	4c6dc7e9957b4a6	3141ef6e2deebac98ceb8b58f683b6d
5	800102006	51491a0863cd4686	广东省广州市永福路2号	67a919ab94d57fe8b	1d480f19a662f7cde4	8ca596ce6759f169146ac1	5d1c8870730203b5c4	3948514	3953243	4729	9c0ed82382f499a	d989f58b261cba582c7e8d52ca30cba
6	800102007	0e8ed5c88639aff9a	广东省广州市科珠路3号	2828967e3228adf4d	e11fd68668c18cf47c	27b8b2a594dc109ce2278	1a7b1eba05123f5fb4a	6198571	6204323	5752	46721c8f06d2563	44190d0dc4008a1f5408b152cea7c1
7	800102008	7989d6a3115c8852a	广东省广州市东风东路4号	0a85a00c8b4823af1	017a3f605b6f7456df	804052a670f23bbed0532	ff0529ecfa1764043663	15360659	15363878	3219	ab3c91f8b284a0a	81b24a5d596bc2dd952a49e398eb64
8	800102009	3858d8dd50a6caecf	广东省广州市达道路5号	7f4383242a6d9ea3d	7a828037e86799bd3	0d02eb5e2b11395fc75b3c	e05482ba1ca6ab9ce4	26752536	26758437	5901	2092b372a85ec2e	74c5f5b4ea130b6bbda8eb943e3c3d
9	800102010	ec9f0e2f21e552e84	广东省广州市海珠区仑头路21号	d4493ba88b7e2e4d	88db280bd13878853	881b77do3567do9da07ob	7557a149b848838o7d	19282705	19287020	4315	6bed286e3ff9309b	1347e1a3ef3089361295a5f5f9e54f17

Edit:   Line   Export/Import:   Line   Li															
▶ 1         800102002         a8d717d3e32bba6b         科学域尖塔山路2号         a6205574d0da1055         eCrb2eeld574bcb77d         40270f7d2acc35ba24ca2e         商用         9921006         9926867         5861         1.2         7033.2           2         800102003         7248abb2d2c857524a         广东省广州市黄埔区科学城科研路3号         8a0b7bad45767244         ca2b5e45914da7501         clf8d943417ba7a194b3b         商用         1121621         1128432         6811         1.2         8173.2           3         800102004         09e2el21de4c5f7b4         广东省广州市黄埔区科学城市中9号科汇金台三         1/246103970851fa42         cbd9c078e9de2cb9f1         af51d51a197b00d0311d0         商用         12651710         226555702         3792         1.2         4550.4           4         800102005         e72ba730b64ef409         广东省广州市永福路2号         67a919ab9457le8b         1480119a6627cde4         8ca596ce6759f169146ac1         军用         3948514         3953243         4729         1         4729           5         800102007         0ebest5c88639aff9a         广东省广州市永福路3号         282889673228ad4d         e1168668c18c47c         2708b22a67V34bc109ce2278         军用         6198571         6204323         5752         1         5752           8         800102008         3858d8d50a6caecf		结	算员	页面	Edit: 🚄 🖶 🖺 Export/Import:	<b>19 18</b>									
2 800102003 7248abb2dc85752fa 「	seq	Ia .		name	address	type	phone	contact	power_type	last_meter_num	meter_num	delta_num	unit_price	total_price	L
3 800102004 09e2e/21de4c5ff704. 广东省广州市黄埔区科学大道中99号科汇金台三 1246f03970851fa42 cbd9c078e9de2cbbf1 af51d51a197b0d0d311d0 商用 22655702 3792 1.2 4550.4   4 800102005 e72ba7d5b6f4ef409 广东省广州市先沿中路1号	<b>▶</b> 1	800102002		a8d717d3e32bba6b	科学城尖塔山路2号	a6205574d0da1055	ec7b2eefd574bcb77d	. 40270f7d2acc35ba24ca29	商用	9921006	9926867	5861	1.2	7033.2	
4 800102005	2	800102003		7248abb2dc85752fa	广东省广州市黄埔区科学城科研路3号	8a0b7bad45767244	ca2fb5e45914de7501	. c1f8d943417ba7a194b3b	商用	1121621	1128432	6811	1.2	8173.2	1
5 800102006 51491a0863cd4686 「东省广州市永福路2号 67a919ab94d57fe8b 1d480f19a662f7cde4 8ca596ce6759f169146ac1 军用 3948514 3953243 4729 1 4729 6 800102007 0e8ed5c88639aff9a 「东省广州市科珠路3号 28289676228adf4d e11f(68668c18c147c 27b8b2a594dc109ce278 军用 6198571 6204323 5752 1 5752 800102008 798906a311fc8852a 「东省一州市东风路4号 0a85a00c8b4823af1 1/13a6f605b452af70f2abbe60532 军用 15360659 153683878 3219 1 3219 8 8 800102009 3858d8d50a6caect 「东省广州市水温路5号 744383242a6d9ea3d 7a828037e86799bd3 0d02eb5e2b11395fc7b3bc 军用 26752536 26758437 5301 1 5901	3	800102004		09e2ef21de4c5f7b4	广东省广州市黄埔区科学大道中99号科汇金谷三	1f246f03970851fa42	. cbd9c078e9de2cb9f1	. af51d51a197b0d0d311d0	商用	22651710	22655502	3792	1.2	4550.4	
6     800102007     0e8ed5c88639aff9a     广东省广州市科珠路3号     2828967e3228adf4d e11fd68668c18cl47c     27b8b2a594dc109ce2278     军用     6198571     6204323     5752     1     5752       7     800102008     7989d6a3115c8852a     广东省广州市东风东路4号     0a85a00c8b4823al1     017a3f605b6f7456df     804052a670f23bbed0532     军用     15360659     15363878     3219     1     3219       8     800102009     3858d8dd50a6caecf     广东省广州市达道路5号     7/4383242a6d9ea3d     7828037e86799bd3     0d02eb5e2b11395fc75b3c     军用     26752536     26758437     5901     1     5901	4	800102005		e72ba7d3b6f4ef409	广东省广州市先烈中路1号	bd79fb3bc0fd1fc193	b27158d621be685dd	5e56dc0a2d45b4163b764	商用	17615139	17623592	8453	1.2	10143.6	1
7     800102008     7989d6a3115c8852a     广东省广州市东风东路4号     0a85a00c8b4823al1     017a3l605b6l7456dl     804052a670l23bbed0532     军用     15360659     15363878     3219     1     3219       8     800102009     3858d8dd50a6caecl     广东省广州市达道路5号     7/4383242a6d9ea3d     7a828037e86799bd3     0d02eb5e2b11395lc75b3c     军用     26752536     26758437     5901     1     5901	5	800102006		51491a0863cd4686	广东省广州市永福路2号	67a919ab94d57fe8b	. 1d480f19a662f7cde4	8ca596ce6759f169146ac1	军用	3948514	3953243	4729	1 🥏	4729	
8 800102009 3858d8d50a6caecf 广东省广州市达道路5号 7/4383242a6d9ea3d 7a828037e86799bd3 0d02eb5e2b11395fc75b3c 军用 26752536 26758437 5901 1 5901	6	800102007		0e8ed5c88639aff9a	广东省广州市科珠路3号	2828967e3228adf4d	. e11fd68668c18cf47c	27b8b2a594dc109ce2278	军用	6198571	6204323	5752	1	5752	300
	7	800102008		7989d6a3115c8852a	广东省广州市东风东路4号	0a85a00c8b4823af1	. 017a3f605b6f7456df	804052a670f23bbed0532	军用	15360659	15363878	3219	1	3219	
9 800102010 639(0e2)(21e552e84 广东省广州市海环区企具整31号 64493ba88b7a2044 98db380bd13879853 881b77da3567da9da07eb 商用 19282705 19287020 4315 12 5178	8	800102009		3858d8dd50a6caecf	广东省广州市达道路5号	7f4383242a6d9ea3d	. 7a828037e86799bd3	. 0d02eb5e2b11395fc75b3c	军用	26752536	26758437	5901	1	5901	1
	9	900102010		ec9f0e2f21e552e84	广东省广州市海珠区企业吸21号	d4493ba88b7e2e4d	88db280bd13878853	881b77de3567de9da07eb	商用	19282705	19287020	4315	1.2	5178	

/	主管领导	页面 □	Edit: 💪 🐯 👺   Export/Import: 🏭 🖔									
seq	id	name	address	type	phone	contact	power_type	last_meter_num	meter_num	delta_num	unit_price	total_price
<b>⊳</b> 1	800102002	广州泰菱科技研发公司	科学城尖塔山路2号	民营企业	(020)32135832	徐文章	商用	9921006	9926867	5861	1.2	7033.2
2	800102003	广州市光机电技术研究院(科研路	) 广东省广州市黄埔区科学城科研路3号	事业单位	(020)32293136	孟建国	商用	1121621	1128432	6811	1.2	8173.2
3	800102004	汤臣倍健	广东省广州市黄埔区科学大道中99号科汇金谷三	民营企业	(020)28956600	王爱军	商用	22651710	22655502	3792	1.2	4550.4
4	800102005	广州军区广州警备司令部	广东省广州市先烈中路1号	军队	(020)85170232	李先民	商用	17615139	17623592	8453	1.2	10143.6
5	800102006	广州军区通讯团	广东省广州市永福路2号	军队	(020)38363171	屈解放	军用	3948514	3953243	4729	1	4729
6	800102007	广州军区防化团	广东省广州市科珠路3号	军队	(020)87775672	李梦	军用	6198571	6204323	5752	1	5752
7	800102008	广州军区后勤部	广东省广州市东风东路4号	军队	(020)38366888	万三强	军用	15360659	15363878	3219	1	3219
8	800102009	广州军区司令部	广东省广州市达道路5号	军队	(020)34068798	王锐	军用	26752536	26758437	5901	1	5901
9	800102010	广东财经大学	广东省广州市海珠区仑头路21号	事业单位	(020)84096494	周斌	商用	19282705	19287020	4315	1.2	5178

# 可搜索加密技术



企业敏感数据外包存储的安全性与可用性同样重要









2000



2013



2014

2013



2016

Sun等结合ABE实现 Du等提出支持关键词 粒度动态查询授权是 DMSSE机制

2020



- 检索与检索结果的访问控制粒度不统一, 检索授权粒度过粗或过细, 缺乏实用性
- 、索引数据膨胀率高,且依赖于内存存储, 难以满足大规模密态数据高效查询检索需求

## 可搜索加密技术



•融合属性加密与可搜索加密的分块数据存储组织技术,实现数据加密存储、密态数据搜索、查询快速响应

索引构建方法 分布式存储 混合查询

大数据中心 大数和和一 大数和于 大面和 大面和 大面和 大面和和一 大面和和一 大面和和一 大面和和一 大面和和一 

查询、验证授权;解密秘钥

单关键字查询 布尔查询 持单关键 验索、布 查询等 定用性

安全性 溶储、传输、计算全过程 加密

• **安全性**:存储、传输、计算全过程加密,支持适配商密、国密等算法 • **可用性**:支持单关键词检索。布尔检索:提供表。列级细粒度访问控制

• 可用性: 支持单关键词检索、布尔检索; 提供表、列级细粒度访问控制策略

• 高性能: 采用索引分块存储方法, 亿级记录规模的密态数据, 单关键词检索

响应时间小于1秒; 索引大小仅为数据的45%

性能 利用索引分 块技术实现 高性能检索

# 共享学习技术

- •共享学习技术是一种在多方参与且互不信任场景下,聚合多方数据并保护数据 隐私和安全,实现数据共享的分布式学习范式
- •共享学习技术在工业界有着广泛的应用前景,有望成为下一代人工智能协同算 法和协作网络的基础



安全合规

满足安全及合规要求 数据不泄露 保证数据和模型安全



联合建模

打破数据孤岛 联合多方建模 聚合数据价值 连接不同场景



#### 提升赋能

合作推动行业 建立激励机制 互利共赢 赋能行业AI





隐私保护深度学 习 CCS15

2015

TEE ML 可信执行环

Microsoft

2016

境, USENIX16

提出联邦学

习, AIStats17

Google

2017

安全多方

计算,82

2006

1980



WeBank 开源框架FATE



提出分裂学习

(Split Learning)

2018

完整 完整 完整 共享学习平台

2019



IEEE标准委员会一致投 票通过联邦学习国际 标准 (IEEE P3652.1)



开源框架PaddleFL



2020

共享学习技术的基本概念



## 共享学习技术



功能	隐私学习	联邦学习	竞合学习	可信机器学习	分裂学习	共享学习	
降维	ig:					$\sqrt{}$	
差分隐私	$\checkmark$	$\checkmark$		It I'm	$\checkmark$	$\checkmark$	
可信计算环境	$\checkmark$		<b>√-</b> /-	\ \/ \	√	$\checkmark$	
安全多方计算	$\checkmark$	$\checkmark$	V		$\checkmark$	$\checkmark$	K
同态加密	$\checkmark$	$\sqrt{}$				$\sqrt{}$	
数据/模型受控	√ / X	4		X / √		VVV	连

安全性

非独立同分布的数据 连接状态不稳定的网络 计算能力不一致的节点 重构攻击

模型反演攻击 成员推理攻击 共享学习作为未来人工智能发展的底层技术,它依靠安全可信的数据保护措施下连接数据孤岛的模式,将不断推动全球 人工智能技术的创新与飞跃。随着共享学习在更大范围和更多行业场景的渗透及应用,它在更高层面上对各类人群、组 织、行业和社会都将产生巨大影响。

共享学习的社会价值

共享学习的商业价值

共享学习的应用场景

加速人工智能技术创新发展

保障隐私信息及数据安全

促进全社会智能化水平提升

带动跨领域的企业级数据合作

催生基于联合建模的新业态和模式

降低技术提升成本和促进创新技术发展

金融风控

视觉安防

自动驾驶

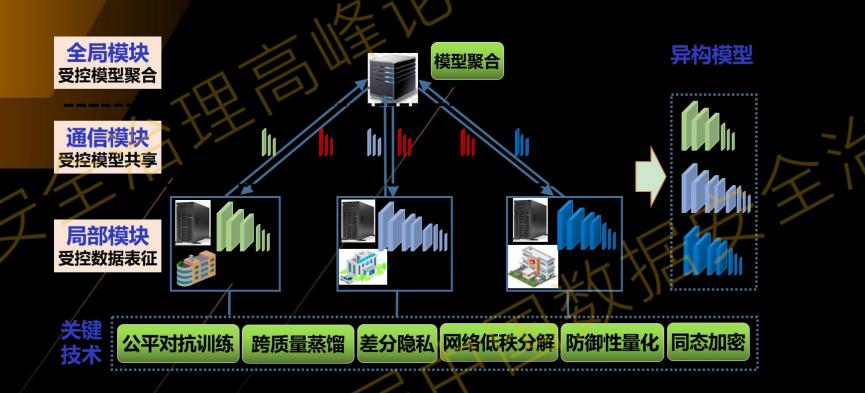
智慧医疗

智慧零售

享学习技术的重大价值

共享学习技术面临的问题和挑战

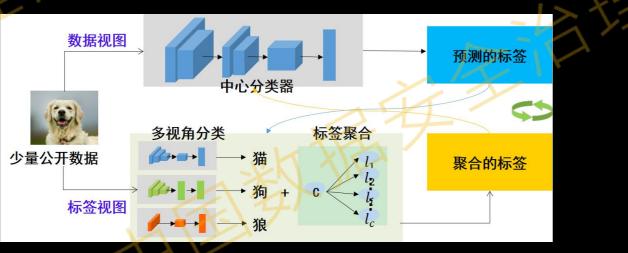
## 共享学习技术



全过程受控的局部-全局协调算法

关键技术:基于耦合视图的数据学习

问题难点:跨组织多源数据共享,异构鸿沟难填技术思路:聚合多视角弱标签,耦合视图联合训练

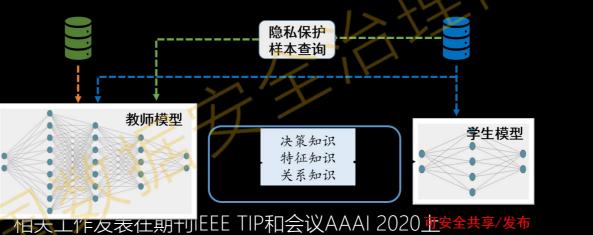


相关工作发表在AAAI 2020上 Coupled-view Deep Classifier Learning from Multiple Noisy Annotators

共享学习若干技术进展

关键技术: 基于知识蒸馏的模型共享

问题难点:模型保障高效知识传递的同时面临隐私泄露 技术思路:教师-学生训练,不直接访问数据下模型传承



Efficient Low-Resolution Face Recognition via Bridge Distillation
Look One and More: Distilling Hybrid Order Relational Knowledge for Cross-Resolution Image Recognition



赋能广泛的数据隐私与算法安全服务

DATA SECURITY GOVERNANCE

# 总结与展望

The state of the s

- •大数据时代/数据安全性与数据可用性同等重要。属性加密、共享学习等技术适用于很多数据共享应用场景,具有很好的应用前景;
- •相关技术在理论研究方面取得了丰硕的成果,相对而言还没有广泛的应用;
- •希望产学研用各方能够加深合作, 共同提升数据安全治理的技术支撑能力。

