申请代码	F0206
接收部门	
收件日期	
接收编号	6187060411

国家自然科学基金

申 请 书

（2 0 1 8 版）

资助类别： 面上项目

亚类说明：

附注说明：

项目名称： 基于访问代理体系结构的密文搜索关键技术研究

申 请 人： 刘川意 **电 话：** 0755-26033775

依托单位： 哈尔滨工业大学

通讯地址： 广东省深圳市南山区西丽大学城哈工大校区G栋612室

邮政编码： 518055 **单位电话：** 0451-86414151

电子邮箱： cy-liu04@mails.tsinghua.edu.cn

申报日期： 2018年02月28日

国家自然科学基金委员会

基本信息

申请人信息	姓　　名	刘川意	性别	男	出生年月	1982年05月	民族	汉族
	学　　位	博士	职称	副教授		每年工作时间（月）		8
	是否在站博士后	否		电子邮箱		cy-liu04@mails.tsinghua.edu.cn		
	电　　话	0755-26033775		国别或地区		中国		
	个人通讯地址	广东省深圳市南山区西丽大学城哈工大校区G栋612室						
	工　作　单　位	哈尔滨工业大学/深圳研究生院						
	主要研究领域							

依托单位信息	名　　称	哈尔滨工业大学		
	联　系　人	赵伟	电子邮箱	kjcjcb@hit.edu.cn
	电　　话	0451-86414151	网站地址	http://kjc.hit.edu.cn/

合作研究单位信息	单位名称

项目基本信息	项目名称	基于访问代理体系结构的密文搜索关键技术研究		
	英文名称	Research on Searchable Encrytion based on Cloud Access Security Broker Architecture		
	资助类别	面上项目	亚类说明	
	附注说明			
	申请代码	F0206.信息安全	F020605.系统安全	
	基地类别			
	研究期限	2019年01月01日 -- 2022年12月31日	研究方向：云安全	
	申请直接费用	80.0000万元		

中文关键词	数据保护；密文搜索；云访问安全代理；云服务协议解析
英文关键词	Data Protection; Searchable Encryption; Cloud Access Security Broker (CASB); SaaS Application Parser

中文摘要	云计算模式下数据所有权和管理权发生分离，如何保护用户敏感和隐私数据，至关重要。可行的思路是数据加密后再上传云端。但是数据加密和云服务功能保全本身是一对矛盾，所以以密文搜索为代表的密文管理及计算，在云和大数据时代将变得愈发重要，近年来也受到工业界和资本的大力追捧。本项目针对目前密文搜索方案需要修改云服务商的接口，且搜索功能有较大退化的问题，提出一种由访问代理执行的密文搜索BESE体系结构，并在此基础上深入研究支撑关键技术，包括:用户敏感数据提取和理解，访问代理执行的数据加解密与密钥管理，索引构建和复杂搜索请求解析，跨访问代理的数据分享等。结合典型的云服务，研发原型系统，进行安全性分析和性能评价。并争取将该原型系统用于实际SaaS应用中，面向云时代有巨量市场价值的云访问安全代理CASB，突破BESE共性关键技术，为国产密文搜索产品化提供支撑。
英文摘要	The division of data ownership and data management is regarded as the key characteristics of cloud computing. How to protect mission-critical data or privacy-sensitive data increases in importance. A promising solution is encryption, providing only encrypted data to the cloud. However, there exists a conflict between encryption and the full functionality in the cloud applications. Thus Searchable Encryption will become a commodity in future cloud era, and in fact it has received intensive attentions from the industry and capital in recent years. However, at present most of the ciphertext search schemes in academia lose some query expressiveness and should modify current cloud Application Programming Interface (API). This project presents a CASB based searchable encryption. And on this basis, it studies the key technologies, including user sensitive data extraction and understanding, data encryption and decryption and key management executed by access broker, index building and advanced query request analysis, data sharing across brokers. Combined with typical cloud applications, this project will develop a prototype system and analysis the security and performance of the system. And we will endeavor to use this prototype system in practical, face to the Cloud Access Security Broker which has a huge market value, break through the common key technologies of BESE, and finally support for converting the Searchable Encryption into product in China.

项目组主要参与者（注：项目组主要参与者不包括项目申请人）

编号	姓名	出生年月	性别	职 称	学 位	单位名称	电话	电子邮箱	证件号码	每年工作时间（月）
1	何慧	1974-04-20	女	教授	博士	哈尔滨工业大学	13895808443	hehui@hit.edu.cn	220202197404202124	8
2	林杰	1987-02-11	男	博士后	博士	哈尔滨工业大学	18810542951	jie_lin@bupt.edu	350881198702110035	8
3	段少明	1994-02-16	男	博士生	硕士	哈尔滨工业大学	13612974476	821197264@qq.com	43052519940216491X	8
4	冯宽	1995-11-17	男	硕士生	学士	哈尔滨工业大学	15736873414	2417406448@qq.com	41272819951117287X	8
5	赵艺茗	1995-03-26	男	硕士生	学士	哈尔滨工业大学	18575513864	1786796646@qq.com	321324199503260036	8
6	郑旭如	1993-10-27	男	硕士生	学士	哈尔滨工业大学	18814122619	953796033@qq.com	440823199310277357	8
7	庄荣飞	1992-06-23	男	硕士生	学士	哈尔滨工业大学	15906060589	316453357@qq.com	350502199206231519	8

总人数	高级	中级	初级	博士后	博士生	硕士生
8	1	1		1	1	4

国家自然科学基金项目资金预算表（定额补助）

项目申请号：6187060411　　项目负责人：刘川意　　金额单位：万元

序号	科目名称	金额
	(1)	(2)
1	**一 、项目直接费用**	80.0000
2	1、 设备费	23.8000
3	(1)设备购置费	23.80
4	(2)设备试制费	0.00
5	(3)设备改造与租赁费	0.00
6	2、 材料费	4.80
7	3、 测试化验加工费	3.80
8	4、 燃料动力费	0.00
9	5、 差旅/会议/国际合作与交流费	8.00
10	6、 出版/文献/信息传播/知识产权事务费	12.80
11	7、 劳务费	18.60
12	8、 专家咨询费	4.20
13	9、 其他支出	4.00
14	**二、 自筹资金来源**	0.00

预算说明书（定额补助）

（请按《国家自然科学基金项目资金预算表编制说明》中的要求，对各项支出的主要用途和测算理由及合作研究外拨资金、单价≥10万元的设备费等内容进行详细说明，可根据需要另加附页。）

设备费：用于处理高并发请求，以及对大规模数据进行加解密，需要高性能GPU服务器2台，以每台9.5万计算，共需19万元。购买升级服务器所用的高性能GPU 6块，以每块0.8万元计算，合计4.8万元。设备费共计23.8万元。

材料费：材料费在执行过程中需要消耗终端机及服务器的配件，需要对实验和开发环境的各种设备进行维修和损坏部件更换。购买打印机硒鼓以及打印纸。材料费总计4.8万元。

测试化验加工费：对BESE架构的密文搜索原型系统访问代理加解密功能和密文搜索功能进行测试，共计3.8万元。

差旅/会议/国际合作交流费：1、对国内相关需求调研所需差旅费；2、3-5次国际会议、学术会议所需费用。

出版/文献/信息传播/知识产权事物费：1、15-20篇论文发表费用；2、相关书籍资料购买费用。

劳务费：本项目参与人员的劳务费用，参与项目人员共8人，合计工作时长224人月，共计18.6万元。

其他费用：项目经费5%（4万元）用于支付项目管理费用。

报告正文

参照以下提纲撰写，要求内容翔实、清晰，层次分明，标题突出。

（一）立项依据与研究内容（4000-8000 字）：

1．项目的立项依据（研究意义、国内外研究现状及发展动态分析，需结合科学研究发展趋势来论述科学意义；或结合国民经济和社会发展中迫切需要解决的关键科技问题来论述其应用前景。附主要参考文献目录）：

1.1 研究意义

根据国际云安全联盟 CSA 报告[1]，数据泄露（Data Breach）是云计算最严重风险。仅 2016 年上半年，就有 974 起披露的数据泄露事件，达 5.54 亿条数据记录[2]。可以说，云服务的推广和有效使用，很大程度取决于云计算的可信性！而其根源在于，**用户失去了对托管在云端数据的直接控制能力**[3, 4]。一个有效的方法是将用户隐私或敏感数据加密以后再传到云上，而服务商只能看到密文，数据控制权完全在用户手中。（注意避免用户密钥在云中存储和使用，否则云管理员可通过特权域得到密钥进而窃取用户数据[5][6]）

但是数据加密和云服务功能保全（Functionality Preservation）是一对矛盾。将加密数据上传到云中，云平台就沦为一个仅支持数据上传和下载的数据池，而无法发挥各种云服务对数据计算、管理和挖掘的优势。因此，以密文搜索（Searchable Encryption）为代表的的密文管理及计算，在云计算和大数据时代将变得前所未有的普遍和重要。

密文搜索技术在学术界其实并不是很新的话题了。早在 2000 年，Dawn Song 等[7]即提出一种可搜索对称密钥加密方案，采用流密码对字符型数据进行加密，然后把加密后关键字在密文中异或运算进行搜索。这种线性搜索方法的缺点是搜索效率很低，且无法应对复杂搜索请求如模糊查询，多关键字查询等。Eu-Jin Goh 等[8]设计了一种基于 Bloom filter 的文档索引，通过对搜索词进行散列映射，判断该搜索词是否在特定文档中。Curtmola 等[9]进而提出了构建明文倒排索引（Inverted Index），再将索引加密后传到云端，与云端密文数据进行关联。近年来，很多学者也在关注如何支持更复杂和动态的搜索请求[10-18]。但是所有上述方案都存在两个致命问题：（1）需要修改云服务商的 API 来调用密文搜索的实现库；（2）无法支持复杂搜索请求，搜索能力（Query Expressiveness）相比现代搜索引擎严重退化[19]。我们把这种体系结构总结为云端执行

的密文搜索 CESE（Cloud Executed Searchable Encryption），其基本流程是：在用户端生成密文和加密索引（如果有索引的话）；将两者传到云端；搜索时，由用户生成查询映射函数（Trapdoor），通过云端根据该映射函数查询加密索引，并返回跟索引项所对应的密文数据。尽管已研究近 20 年，但不得不说，仍是学者自娱自乐的状态，更像学术界的“数学游戏”[20]。

与之形成鲜明对比的是：近年来，云访问安全代理 CASB（Cloud Access Security Broker）[21] 受到了工业界和资本的广泛追捧，在 RSA 2016、2017 连续成为整个行业关注的焦点，并连续被 Gartner 评为网络安全 10 大创新性技术之首。Gartner 报告指出，从 2012 到 2020 年，部署 CASB 的云服务用户将从 1%上升到 85%，安全访问成本会随之下降 30%，CASB 市场价值有望达到千亿规模。以 Skyhigh Networks [22]和 Ciphercloud [23]为代表的“独角兽”创新企业也推出基于 CASB 架构的密文搜索商业产品，宣称可实现与云服务商透明的密文搜索。基于访问代理执行搜索的结构，使数据加解密、密文搜索与云服务商解耦合，且能克服云端执行搜索所固有的实用性缺陷。

然而，并不是把结构一改，所有问题就都天然解决了。随着向真实部署和实用迈进，很多技术挑战和研究机会又反馈回学术界。总结起来，主要是以下方面：如何解决密文搜索算法跟众多云应用无缝适配、数据提取与解析等**体系结构**问题；如何解决**搜索功能与数据加密强度的矛盾**问题；如何解决**多用户数据上传、分享和搜索**问题。

回答和解决这些问题，需要融合密码学、系统结构、协议分析和软件工程，进行深入研究和探索。

1.2 国内外研究现状及发展动态

通过对密文搜索相关研究工作进行系统梳理和对比分析，将相关工作划分为体系结构、复杂搜索能力的支持、安全性及攻击、多用户支持等 4 个类别，整体对比分析如表 1 所示。

- **密文搜索体系结构**

在“研究意义”中已经介绍和分析，密文搜索按体系结构可以分成云端执行的密文搜索和访问代理执行的密文搜索。前者由云端实现加密索引查询（往往通过查询映射函数 Trapdoor），由云端负责关联密文索引和密文数据，实施搜索。这些数据结构都必须对特定的搜索请求事先固定好，不能同时满足多种高级搜索功能，且需要修改云应用服务器端 API，大大限制了在实际应用场景落地的可能。后者通过引入云访问代理，把原来通过客户端软件执行的数据加解密和元数据（包括密钥）管理，上位到由访问代理执

行。目前主要是偏计算机系统结构和系统安全的学者在研究： CryptDB [24]访问代理位于图 2c 点，针对 mysql 关系数据库实现 sql 查询重解析的密文搜索；Mylar [25]访问代理位于图 2b 点，通过提供一种新的 web 框架，由应用自动调用该框架的编程 API 保证用户数据在加密同时可搜索；ShadowCrypt [26]访问代理位于图 2a 点，通过识别、加密用户在网页文本框中的输入，并通过 Trapdoor 密文匹配实现密文搜索；M-Aegis [27]通过提出网络协议栈 7.5 层，提取手机终端 UI 界面的输入，并通过构建索引，实现密文搜索。

在云计算加速普及的形势下，各类云服务种类繁多，且直接导致了云数据类型的多样化，不同类别的数据对加密要求和搜索要求也不尽相同。同时，密文搜索如何从现有云服务提取数据、敏感数据解析等，都是体系结构的研究空间。

表 1 密文搜索相关工作对比与分析

体系结构	文献或系统	模糊匹配	多关键字	智能排序	动态更新	无需修改云服务端	多用户	支持对明文标准加密	支持对索引标准加密	支持数据类型
云端执行搜索	SWP [7]	×	×	×	×	×	×	×	-	文本
	Goh [8]	×	×	×	✓	×	×	✓	×	文本
	Curtmola [9]	×	×	×	×	×	✓	✓	✓	文本
	GDFS [10]	×	✓	✓	×	×	×	✓	×	文本
	Wang [11]	✓	×	×	×	×	×	✓	×	文本
	Cash [12]	×	×	×	✓	×	×	✓	✓	文本
代理执行搜索	CryptDB [24]	×	×	×	✓	✓	×	×	×	SQL 数据库
	Mylar [25]	×	×	×	✓	✓	✓	✓	×	文本
	ShadowCrypt [26]	×	✓	×	✓	✓	×	✓	-	网页输入框数据
	M-Aegis [27]	×	×	×	✓	✓	×	×	×	Andriod UI 页面
	本项目方案	✓	✓	✓	✓	✓	✓	✓	✓	网页输入框、富文本、二进制流

- **复杂搜索能力的支持**

密文搜索对复杂搜索能力的相关工作主要集中于三种搜索请求，即多关键字排序搜索（一次查询可包含多个关键字，对所有文档查询后返回具有和查询向量最相关的文档集合），模糊搜索（当关键字拼错或格式有误时，仍能找到近似的关键字进行搜索）和动态更新（可以添加或删除可搜索的加密文件）。

Xia 等人[10]提出了一种基于树的多关键字排序搜索方案，满足亚线性搜索时间，但

泄漏了访问模式和一定量的相关性；Li 等人[28]]通过预先设定各关键字基于通配符的模糊集合来构建模糊搜索方案。此方案允许加密索引泄漏一定的编辑距离信息；Kamara 等人[29]设计动态更新机制，需要维护复杂的数据结构。该方案泄漏搜索模式和访问模式，并且在更新过程中泄露了某些关键字出现在特定文档中的信息。

国内学者也对密文搜索功能开展研究：彭等[13]提出一种基于 B+树构建的安全密文全文索引结构的全文检索系统；冯等[14]提出使用 Bloom filter 为文档关键词构造索引；吴等[15]设计了一种基于搜索历史的密文检索系统，可对搜索结果进行相关性排序；卢等[16]针对文本文件，将文档和索引分开加密和关联； 马等[17]利用身份加密技术提出了无证书连接关键字密文搜索方案；钮等[18]针对数值型和字符型密文，分别提出数值顺序置换和特征过滤的方法实现范围检索和关键字检索。

由上可知，对于每个搜索功能，以上密文搜索方案需要生成一个特定结构的索引，用户需要生成特定的陷门，然后云端可以使用特定的算法对加密的索引执行特定的查询。它们给云端应用程序带来了额外的负担，同时在一个加密索引上实现多个功能是不切实际的。

- **安全性分析及典型攻击**

表 2 总结了针对密文搜索的典型风险和攻击方案。IKK [30]首先利用模拟退火算法[31]对密文搜索泄露的搜索模式和访问模式进行攻击。当明文信息不准确或只有部分明文已知时，IKK 查询恢复成功率较低。CGPR [32]提出了计数攻击算法，而不使用优化算法。然而，CGPR 要求攻击者知悉被攻击者文档的全部信息才能达到较高的查询恢复率。当只知道文档集的一部分（例如，小于 80%）时，IKK 和 CGPR 攻击的查询恢复率都接近于 0。Shadow Nemesis [33]针对基于令牌的密文搜索方案进行攻击。然而它没有利用部分知识发起查询恢复攻击，在已知部分文档的情况下此方案获得的查询恢复成功率也很低。ZKP [34]使用主动攻击来推断查询陷门对应的明文信息。当用户只加密和索引自己上传的敏感数据时，此攻击条件难以满足。

表 2 针对密文搜索的不同攻击方案比较

攻击方案	攻击算法	成功率高	攻击目标
IKK[30]	模拟退火	所有文档	基于加密索引或令牌
CGPR[32]	计数攻击	所有文档	基于加密索引或令牌
ZKP[34]	文档注入	主动攻击	基于加密索引或令牌
Shadow Nemesis[33]	图匹配	所有文档	基于令牌

- **多用户使用场景**

密文搜索方案按照数据发送者和数据接收者对应情况可划分为单用户写/单用户读（S/S）、多用户写/单用户读（M/S）、单用户写/多用户读（M/S）及多用户写/多用户读（M/M）。

大多数基于对称加密的密文搜索方案[7-9]仅支持单用户读写文件，即用户仅能搜索自己上传的加密文档。PEKS 方案[35]使用非对称加密生成加密索引。文档的每个关键字使用用户的公钥加密成密文，并附加到加密文档的后面。这样，多个用户可以使用某用户的公钥生成加密索引，只有拥有对应私钥的用户才能生成合法的查询陷门来搜索加密索引。这种方案带来很高的时间开销。Liu 等人[36]提出了基于 PEKS 的密文搜索（SPKS）方案，允许云服务提供商参与部分解密，而不需要知道明文的具体内容。

为了支持单用户写/多用户读或多用户写/多用户读，密文搜索方案需要引入分发密钥的机制，以允许多个用户搜索加密数据。常用的分发密钥机制[37-38]包括密钥分享，密钥分发，代理重加密等其他技术。另外，多用户方案的另一个重要需求是用户撤销问题[9,39]，即允许增加或删除一个用户搜索某加密索引的权限。密文搜索用户撤销机制多结合基于属性的加密[40-42]实现。

1.3 主要参考文献

[1] C. S. Alliance, “CSA’s Cloud Computing Top Threats in 2016” Cloud Security Alliance, Top Threats Working Group, February 2016. Available: https://downloads.cloudsecurityalliance.org/. assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf.

[2] BREACH LEVEL INDEX, “It’s All About Identity Theft” BreachLevelIndex, 2016. Available: http://breachlevelindex.com/assets/Breach-Level-Index-Report-H12016.pdf.

[3] Y.Chen, V.Paxson, R.Katz. What’ s New About Cloud Computing Security? Technical Report UCB/EECS-2010-5, Berkeley, 2010.

[4] R.K.L.Ko, P.Jagadpramana, M.Mowbray, S.Pearson, M.Kirchberg, Q.Liang, B.S.Lee. TrustCloud: A framework for accountability and trust in cloud computing, in 2nd IEEE Cloud Forum for Practitioners. IEEE Press, 2011.

[5] Bouche J, Kappes M. Attacking the Cloud from an Insider Perspective. Proceedings of the International Conference on Cloud Technologies and Applications (CloudTech). Marrakech, Morocco, 2015: 175-180.

[6] Rocha F, Correia M. Lucy in the sky without diamonds: Stealing confidential data in the cloud. Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks. Hong Kong, China, 2011: 129-134.

[7] SONG D X, WAGNER D, PERRIG A. Practical techniques or searches on encrypted data. Proceedings of the IEEE Symposium on Security and Privacy. CA, USA, 2000.36-49.

[8] Eu-Jin Goh. Secure indexes. In proceedings of the 2004 Workshop on Information Security Applications. Jeju Island , Korea, 2004. 7(15): 73-86.

[9] Curtmola R, Garay J, Kamara S, et al. Searchable symmetric encryption: Improved definitions and efficient

constructions. Journal of Computer Security, 2011, 19(5):79-88.

[10] Xia Z, Wang X, Sun X, et al. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data[J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 27(2): 340-352.

[11] Wang, Bing, et al. Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud. INFOCOM, 2014 Proceedings IEEE. IEEE, 2014.

[12] Cash D, Jaeger J, Jarecki S, et al. Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation[C]//NDSS. 2014, 14: 23-26.

[13] 宋伟, 彭智勇, 王骞, 等. Mimir: 一种基于密文的全文检索服务系统[J]. 计算机学报, 2014, 37(5): 1170-1183.

[14] 惠榛, 冯登国, 张敏, 等. 一种可抵抗统计攻击的安全索引[J]. 计算机研究与发展, 54(2): 295-304.

[15] 谢贤明, 吴庆波, 谭郁松. 基于搜索历史的密文检索系统研究[J]. 中国电子商情: 通信市场, 2011 (4): 99-104.

[16] 彭霖, 李瑞轩, 宋赛, 辜希武, 文坤梅, 卢正鼎. 一种密文全文检索系统的安全索引结构[J]. 微电子学与计算机, 2012, 29(9):27-30.

[17] 伍祈应, 马建峰, 李辉, 苗银宾. 无证书连接关键字密文检索[J]. 西安电子科技大学学报. 2017(03)

[18] 刘念, 周亚建, 钮心忻, 等. XML 数据库的加密与密文检索[J]. 北京邮电大学学报, 2010, 33(2):105-110.

[19] Bösch C, Hartel P, Jonker W, et al. A survey of provably secure searchable encryption. ACM Computing Surveys (CSUR), 2015, 47(2): 18.

[20] Alexandra Boldyreva. Searching Encrypted Cloud Data: Academia and Industry Done Right. Technical Report from School of Computer Science, Georgia Institute of Technology. Feb 2015. From: https: //www.slideshare.net/ skyhighnetworks/searching-encrypted-cloud-data-academia-and-industry-done-right

[21] Gartner Report. How to Evaluate and Operate a Cloud Access Security Broker. December 8,2015.

[22] Skyhigh Networks. https://www.skyhighnetworks.com/.

[23] CipherCloud. https://www.ciphercloud.com/.

[24] Popa R A, Redfield C, Zeldovich N, et al. CryptDB: protecting confidentiality with encrypted query processing[C]//Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles. ACM, 2011: 85-100.

[25] Popa R A, Stark E, Valdez S, et al. Building web applications on top of encrypted data using Mylar[C]//11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14). 2014: 157-172.

[26] He W, Akhawe D, Jain S, et al. Shadowcrypt: Encrypted web applications for everyone[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014: 1028-1039.

[27] Lau B, Chung S, Song C, et al. Mimesis aegis: A mimicry privacy shield–a system's approach to data privacy on public cloud// Proceedings of the 23rd USENIX Security Symposium. SanDiego California, USA, 2014: 33-48.

[28] Li J, Wang Q, Wang C, et al. Fuzzy keyword search over encrypted data in cloud computing[C]//INFOCOM, 2010 Proceedings IEEE. IEEE, 2010: 1-5.

[29] Kamara S, Papamanthou C, Roeder T. Dynamic searchable symmetric encryption[C]//Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012: 965-976.

[30] Islam M S, Kuzu M, Kantarcioglu M. Access Pattern disclosure on Searchable Encryption: Ramification, Attack and Mitigation[C]//NDSS. 2012, 20: 12.

[31] S. Kirkpatrick, C. Gelatt, and M. Vecchi. Optimization by simulated annealing. Science, 220(4598):671–679, May 1983.

[32] Cash D, Grubbs P, Perry J, et al. Leakage-abuse attacks against searchable encryption[C]//Proceedings of the

22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015: 668-679.
[33] Pouliot D, Wright C V. The shadow nemesis: Inference attacks on efficiently deployable, efficiently searchable encryption[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 1341-1352.
[34] Zhang Y, Katz J, Papamanthou C. All Your Queries Are Belong to Us: The Power of File-Injection Attacks on Searchable Encryption[J]. IACR Cryptology ePrint Archive, 2016, 2016: 172.
[35] Boneh D, Di Crescenzo G, Ostrovsky R, et al. Public key encryption with keyword search//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques.Berlin Heidelberg,Germany, 2004: 506-522
[36] Liu Q, Wang G, Wu J. Secure and privacy preserving keyword searching for cloud storage services. Journal of Network and Computer Applications, 2012, 35(3):927–933.
[37] Peishun Wang, Huaxiong Wang, and Josef Pieprzyk. 2007b. Common secure index for conjunctive keywordbased retrieval over encrypted data. In SDM (LNCS), Vol. 4721. Springer, 108–123.
[38] Changyu Dong, Giovanni Russello, and Naranker Dulay. 2008. Shared and searchable encrypted data for untrusted servers. In DBSec. Springer-Verlag, Berlin, Heidelberg, 127–143. DOI:http://dx.doi.org/10.1007/978-3-540-70567-3_10.
[39] Yanjiang Yang, Haibing Lu, and Jian Weng. 2011. Multi-User private keyword search for cloud computing. In CloudCom. IEEE, 264–271.
[40] Sahai A, Waters B. Advances in Cryptology–Eurocrypt: Fuzzy identity-based encryption. Berlin Heidelberg: Springer, 2005.
[41] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data//Proceedings of the 13th ACM Conference on Computer and Communications Security. Virginia Alexandria, USA, 2006: 89-98.
[42] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy Attribute-Based Encryption//Proceedings of the 2007 IEEE Symposium on Security and Privacy. Oakland California, USA, 2007:321-334.
[43] Liu Chuanyi, Wang Guofeng, Han Peiyi, Pan hezhong, Fang Binxing. A Cloud Access Security Broker Based Approach for Encrypted Data Search and Sharing[C]// International Conference on Computing, NETWORKING and Communications. IEEE, 2017.
[44] Han P, Liu C, Fang B, et al. Revisiting the Practicality of Search on Encrypted Data: From the Security Broker's Perspective[J]. Scientific Programming, 2016, 2016.
[45] 刘川意等. 云计算环境下密文搜索算法的研究[J]. 通信学报, 2013, 34(7): 143-153.
[46] 王国峰, 刘川意等. 云计算模式内部威胁综述[J]. 计算机学报, 2017, 40(2): 296-316.
[47] 王佳慧, 刘川意等. 面向物联网搜索的数据隐私保护研究综述[J]. 通信学报, 2016, 37(9):142-153.

2. 项目的研究内容、研究目标，以及拟解决的关键科学问题（此部分为重点阐述内容）；

2.1 研究目标

在云和大数据时代密文搜索愈发重要的背景下，针对目前密文搜索需要对云服务的API做根本修改，搜索功能严重退化等问题，深入研究密文搜索体系结构，提出基于双向映射倒排索引的复杂搜索算法，多用户上传与搜索的跨代理数据分享技术等，拟解决

搜索功能与数据加密强度的矛盾、多用户支持等重要研究和技术挑战。并采用构建原型系统来验证和促进关键技术的方法，以期在此领域获得若干共性关键技术的突破，为接下来全自主知识产权相关网络安全系统的应用推进打下坚实基础。

2.2 研究内容

为完成上述研究目标，主要研究内容包括：基于访问代理的密文搜索体系结构，基于双重映射倒排索引的复杂搜索请求支持与安全性，支持多用户上传与搜索的跨代理数据分享技术，以及原型系统研发与评价，其相互关系如图 1 所示。

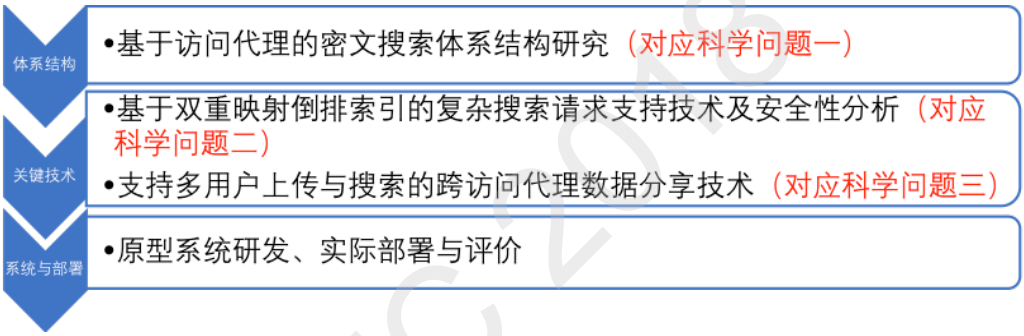


图 1 主要研究内容的相互关系

(1) 基于访问代理的密文搜索体系结构研究

体系结构研究主要解决密文搜索的可部署和可实用性问题。我们总结了数据加解密在云计算体系结构中可能的实现位置，如图 2 所示。只有明确了密文搜索体系结构，才能在此基础上设计相应数据加解密算法和密文搜索请求解析。拟系统分析和比较不同密文搜索体系结构对搜索功能的支持能力、搜索的性能、数据加密的安全强度等。

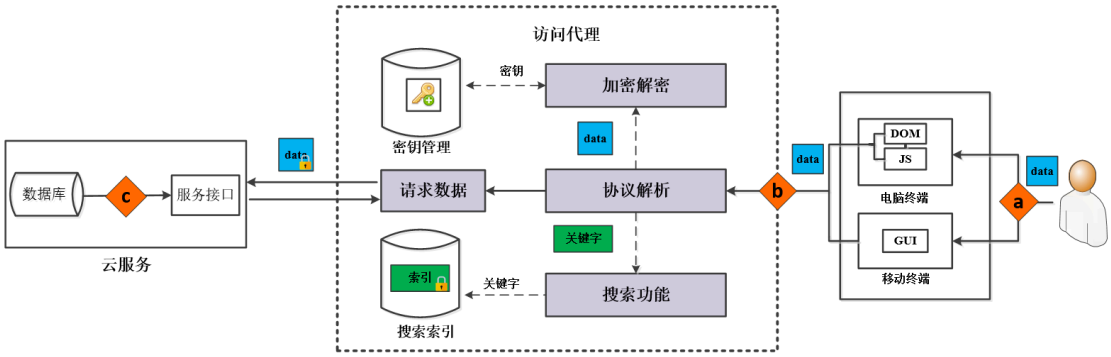


图 2 云计算体系结构中，数据加解密的可能位置（位置 a，b，c）

让密文搜索可用，必须面对一个挑战：众多 SaaS 云服务，若人工逐个分析云服务协议并适配，不仅工作量巨大而且容易出错，因此体系结构研究的另一方面要研究可自动化或半自动化的数据解析与云服务协议适配。在云计算加速普及的形势下，各类云服务种类繁多，且直接导致了云数据类型的多样化，不同类别的数据对加密要求和搜索要求也不尽相同。表 3 列举了常见的云服务，及对应的用户数据类型，加密和搜索要求。例如，CRM 应用中的特定格式数据（如手机号、身份证号）需要在加密的同时保证格式且支持模糊搜索；邮件应用中内含多媒体链接的富文本数据直接加密则会使得邮件服务商无法正常解析富文本格式从而影响应用功能，这种数据的加密需要保证富文本格式且支持动态搜索、含多关键词逻辑的连接搜索等高级搜索功能。拟研究对网页文本框中的输入数据、富文本、文件和二进制流数据等多种类型云数据的提取和理解；研究自动化识别和适配云服务协议；研究用户敏感数据的自动提取、标记，进而加解密。

表 3 典型云服务和对应的数据类型，以及对加密和搜索的要求

应用类别	典型应用	数据类别	加密要求	搜索要求
邮箱应用	QQ 邮箱	文本	通用加密	高级搜索
		富文本	保证格式加密	高级搜索
		文件	流式加密	高级搜索
云存储应用	百度网盘	文件	流式加密	高级搜索
		二进制流数据	流式加密	高级搜索
CRM 应用	纷享销客	特定格式文本框输入数据	保证格式加密	模糊搜索 多关键字搜索
ERP 应用	今目标	特定格式文本框输入数据	保证格式加密	模糊搜索 多关键字搜索
社交应用	微博	限制长度的输入数据	保证长度加密	模糊搜索 多关键字搜索

(2) 基于双重映射倒排索引的复杂搜索请求支持技术及安全性分析

目前密文搜索方案往往需要对标准加密算法进行异化和固化，如为实现密文匹配，将对称加密算法中的初始化向量 IV 固定不变，从而把随机加密变成了确定性加密，代价是降低了加密算法的强度。本项目拟研究一种支持标准通用加密算法的密文搜索，从而在实现搜索功能的同时保证数据加密的安全性。

初一想，这是矛盾的任务，即使同样的明文用标准加密后也会变成不同密文，如此则没法搜索了。因此本项目关键在于：由访问代理解析到要加密的数据后，对其建立搜索索引，然后使用标准加密算法对数据加密，并维护密文数据与加密密钥的映射关系以便搜索。

另一方面，云端执行搜索因本地不存储任何索引，而将索引加密存储到云端，并通过查询单射函数（Trapdoor）将搜索关键词与云端的密文索引进行关联，Trapdoor 无法动态变化和扩展，导致无法支持复杂的搜索请求。

本项目拟研究：基于访问代理的索引构建和复杂搜索请求解析，元数据与云端密文数据的关联映射，实现模糊搜索、多关键字智能排序搜索、动态搜索等复杂搜索的保全。拟设计实现与现代搜索引擎（如 ElasticSearch，Zettair，Sphinx 等）同等水平的各类复杂搜索请求，包括：模糊搜索、含多关键词逻辑的连接搜索、动态搜索等；加密强度可支持主流标准加密算法，如：AES-256，RSA，SM2，SM4 等。

(3) 支持多用户上传与搜索的跨访问代理数据分享技术

云服务上仅仅存储用户的密文数据，用户查看密文数据需要通过访问代理的解密。实际应用场景下，身处不同访问代理之间的用户存在分享密文的需求；用户自身也可能由于工作原因从某一访问代理迁移到另一访问代理，用户希望访问原访问代理加密的数据。因此访问代理之间密文数据的分享是基于访问代理架构的密文搜索亟待解决的新问题。解决这一问题的关键是解决访问代理之间密钥的分享。本项目拟在实现加密解密和密文搜索功能基础上，深入研究访问代理之间，用户数据分享的应用场景，拟定可行的解决方案并完成方案的实现。

(4) 原型系统研发、实际部署与评价

原型系统研发与评价分三步进行：

第一步，设计和实现安全访问代理，并选定若干典型 SaaS 应用，依据本项目提出的基于访问代理的加密、解密流程、密文搜索流程，实现该应用的密文搜索功能。测试和评价功能有效性；定量测评引入的额外开销，具体包括构建索引时间、搜索时间、更新数据时间、索引存储空间、更新数据所用空间、跨访问代理分享数据时间等开销代价；

第二步，在上述基础上，进一步突破自动化敏感数据提取技术、跨访问代理的数据分享。并争取将该原型系统适用于实际典型 SaaS 应用上，突破 CASB 共性关键技术，为国内密文搜索产品化提供支撑。

第三步，研究建立安全分析模型，从密文搜索体系结构的攻击面，加密算法强度分析，密钥和元数据在数据动态更新时的泄露和利用等维度进行深入安全性分析；针对本项目方案中数据加解密、构建索引、搜索等关键环节可能会出现的攻击方式进行深入分析和评价。

2.3 拟解决的关键科学问题

- **问题一、密文搜索的可部署、可实用性问题**

目前密文搜索算法需要修改云服务商的接口，且搜索功能有较大退化。若不解决上述问题，则直接否定了密文搜索的可实用性。而这是大数据和云计算场景对数据保护的迫切需求，也是工业界对学术界的“倒逼”。

- **问题二、搜索功能与数据安全强度的矛盾问题**

搜索功能与安全强度指标往往是相互掣肘和矛盾的，如：若加密的强度和随机性足够高，则对密文的搜索能力相应会退化。绝大多数密文搜索往往采用关键词替换（Tokenization）、初始向量 IV 固定的方式实现安全强度和搜索能力的折衷。而这对矛盾解决的好坏从根本上决定了密文搜索研究的好坏。

- **问题三、密文搜索对多用户的支持度问题**

若仅能做到自己的数据自己上传，自己搜索，则跟云计算的多租户、大数据的共享性要求，存在巨大鸿沟，这是对密文搜索的迫切要求。

3. 拟采取的研究方案及可行性分析（包括研究方法、技术路线、实验手段、关键技术等说明）；

本项目的总体技术路线是：基于访问代理执行的密文搜索体系结构，以自主技术和原创研究为导向，设计实现与现代搜索引擎（如 ElasticSearch，Zettair，Sphinx 等）同等水平的各类复杂搜索请求，包括：模糊搜索、含多关键词逻辑的连接搜索、动态搜索等，加密强度可支持主流标准加密算法，深入研究跨代理的密钥交换和数据分享，完成多用户数据上传和多用户密文搜索，并将上述关键技术形成原型系统，在真实场景中部署和应用。

对应于主要研究内容，从以下三个方面说明研究方案的可行性和特点：

(1) 基于访问代理的密文搜索体系结构

绝大多数云服务使用 Http 或 Https 协议，通过深入分析，用户向云端提交的敏感数据往往在 Http Request 数据包主体中，而用户从云端下载的敏感数据往往在 Http Response 响应主体中。不失一般性，以一个典型的 Web Mail 云服务为例，如图 3 所示，网页加载以后，自动检测出所有的文本输入框，提示用户可以选择要加密的内容并对这些加密项进行标记。之后访问代理识别云服务协议内容中的标记，提取敏感数据并形成加密匹配规则。而对于文件和二进制流数据，访问代理可通过识别传输协议进而解析得到文件和二进制流数据。将上述流程根据云服务、数据类型和格式进行抽象，即可实现

自动识别和提取用户敏感数据。

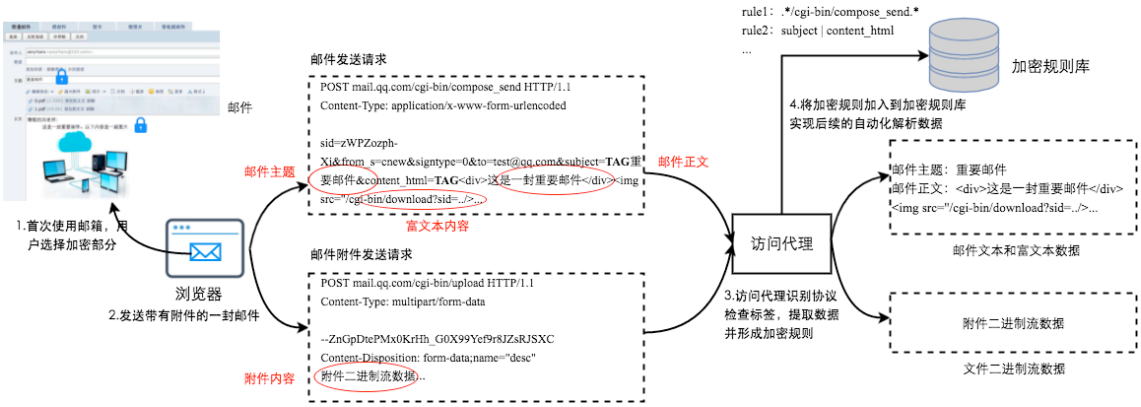


图 3 用户敏感数据的自动化提取和理解

(2) 基于双重映射倒排索引的复杂搜索请求支持技术及安全性分析

解决搜索功能与加密强度矛盾的关键是把原来通过客户端软件执行的数据加解密和元数据（包括密钥）管理，上位到由访问代理执行，如图 4 所示，其引发新的技术挑战包括：当访问代理解析到要加密的数据后，对其建立搜索索引，然后使用标准加密算法对数据加密，并维护密文数据与加密密钥的映射关系。当用户通过访问代理从云端获取密文数据时，访问代理提取密文数据的元数据关联得到对应的密钥，使用密钥解密数据并把明文数据返回给用户。

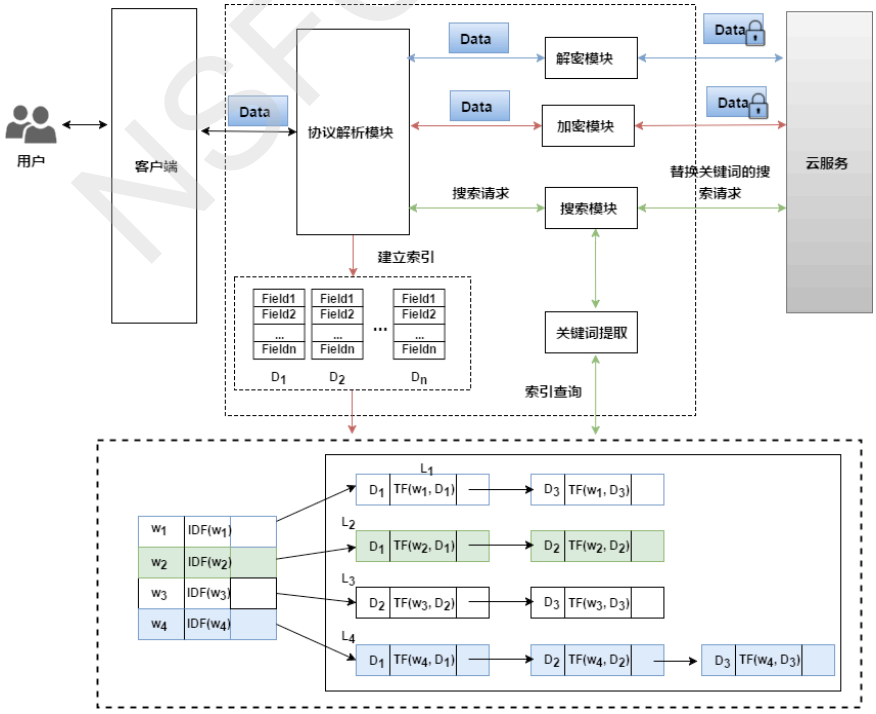


图 4 基于双重映射倒排索引的复杂搜索请求支持框架和主要数据结构

对于搜索索引的建立有两种思路：一是对输入数据分词处理后得到关键字序列，使用标准加密算法加密输入数据得到密文数据，并附上关键字序列对应的多个随机字符串

一起发送给云端；二是建立明文倒排索引并关联云端密文数据。前者通用性好，但功能简单；后者可以支持高级搜索功能，但需要建立索引和密文数据的关联。当用户发起搜索请求时，访问代理解析得到搜索关键字并对索引进行搜索，得到相应的搜索结果。

在本地索引上使用相关搜索算法实现高级搜索功能，如多关键字搜索、模糊查询、动态更新等。在复杂搜索请求解析方面，本项目也做了大量准备，以多关键字可排序搜索为例，初步设计算法如表 4 所示，其中 TF 表示某一文档中某一关键字的频率，IDF 表示某一关键字的逆向文档频率。

表 4 多关键字可排序密文搜索算法

算法：多关键字密文搜索

Input: Keywords Query Vector **Q**, Number **K**

```
1  float RScores[N] = 0;
2  Initialize Length[N];
3  for each w_i ∈ Q
4      get IDF(w_i) and fetch postings list L_wi for W_i;
5      for 1 ≤ j ≤ |D(W_i)|:
6          get node N_i,j = <id(D_i,j) || TF(w_i, id(D_i,j))>;
7          do RScores[id(D_i,j)] += TF(w_i, id(D_i,j)) × IDF(w_i);
8  return Top K components of RScores[N];
```

给定一个密文搜索方案，A 表示一个有状态的概率多项式时间（PPT, Probabilistic Polynomial-Time）攻击者，S 是一个有状态的 PPT 模拟器，L_1 和 L_2 是在 *Ideal* 安全游戏中有状态的泄露函数，s 表示安全参数。定义 $Real_A(s)$ 和 $Ideal_{A,S}(s)$ 游戏如下：

$Real_A(s)$：挑战者根据安全参数 s 产生密钥 k。A 给定数据文件 D，挑战者利用数据 D 和密钥 k 产生加密的索引 I 和加密数据 C，并将 I 和 C 发送给攻击者。然后攻击者进行多项式数量的自适应查询 Q，其中对于每个查询 q 对应的关键字 w，攻击者都会从挑战者处接收到关键字对应的搜索陷门 TD，最后 A 返回一个比特 b 作为游戏的输出。

$Ideal_{A,S}(s)$：A 输出数据文件 D。给定 $L_1(D)$，S 产生并发送 (I^*, C^*) 到 A。然后攻击者进行多项式数量的自适应查询 Q，对于每个查询 q 对应的关键字 w，模拟器接收 $L_2(D, w)$ 并返回对应的陷门 TD^*。最后，A 返回一个比特 b 作为游戏的输出。

如果对于任意 PPT 攻击者 A，任意多项式 p 和足够大的 s，存在一个 PPT 模拟器 S，满足如下条件：

$$|Pr[Real_A(s)=1] - Pr[Ideal_{A,S}(s)=1]| < 1/p(s)$$

则密文搜索方案对于自适应攻击 CKA2 是 (L_1, L_2) 安全的。用同样的方法可定义密文

搜索方案对于非自适应攻击 CKA1 是(L_1, L_2)安全的，但 A 必须在游戏开始时就已经选好了所有的查询 Q，即客户的查询独立于搜索索引和以前的查询结果。

在基于访问代理的密文搜索的查询过程中，对于自适应攻击 CKA2：

（1）L_1 安全性：由于数据通过安全强度高的对称加密方式加密，故攻击者很难从密文中获取额外的信息。由于索引是在访问代理处产生和保存，故攻击者无法获得索引，从而保证了索引的安全性，使攻击者无法获得更多的信息。

（2）L_2 安全性：在搜索过程中，查询关键字交给访问代理，并在访问代理处执行查询，从而向云端隐藏了搜索模式。当执行查询获得搜索结果（文档标识符列表）后，用户向云服务器发送其它请求以检索特定文档。这些请求可以嵌入到其他的检索中，从而混淆了搜索请求和密文检索请求之间的相关性，使云服务器不能得出一次查询请求对应于哪些文件，从而一定程度上向云端隐藏了访问模式。

本项目的密文搜索算法在查询过程中一定程度隐藏了搜索模式和访问模式，所以即使攻击者拥有加密文件对应的所有明文，也不能推理得到查询对应的明文关键字。

(3) 支持多用户上传与搜索的跨访问代理数据分享技术

密文数据分享的本质是密钥交换和分享，拟引入第三方控制节点解决跨代理的密钥分享问题。为了让解决方案更有实际意义，我们假设控制节点也是不可信的（即控制节点可能泄露加密密钥）。因此，拟设计一种双重加密（基于身份加密+非对称加密）实现密钥分享，其初步结构和流程设计如图 5 所示。

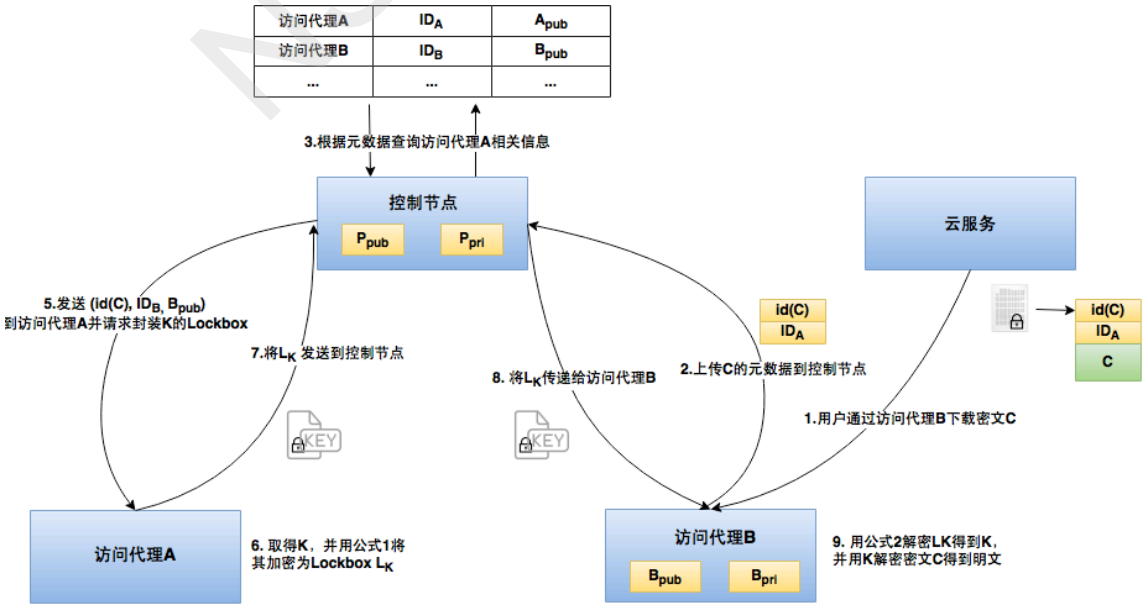


图 5 基于双重加密技术的跨访问代理数据分享结构与主要流程

其中，每个访问代理拥有自身的非对称公私钥对（例如访问代理 B 拥有公钥 B_{pub} 和私钥 B_{pri}），控制节点则为每个代理签发与其 ID 对应的 IBE 私钥（例如访问代理 B

的 ID_B 对应私钥 d_B）。

访问代理 B 下的用户想要查看访问代理 A 下用户上传到云上的数据，首先 B 从云服务上下载密文数据 C 和与 C 相关的元数据（包括 C 的密文 id(C)和加密该密文的代理 ID）。B 将 C 的元数据上传到控制节点，控制节点查询代理信息列表，得到相关数据，确认加密 C 的代理 A，并将 id(C)、B 的公钥 B_{pub} 和 ID_B 发送给代理 A。A 接收到上述数据，根据 id(C)取得对应的密钥 K，利用公式 1 将其加密为 L_K 返回给控制节点。控制节点将其返回给访问代理 B。此时，访问代理 B 利用公式 2 解密得到 C 的密钥 K，则可解密密文，即：

$$L_K = E_{Bpub}(E_{IDB}) \quad (1)$$

$$K = D_{dB}(D_{Bpri}(L_K)) \quad (2)$$

要顺利完成本项目研究工作，需要把传统意义上相对独立的若干研究方向完全打通，包括：密码学，云计算体系结构，计算机系统等，并真正实现协同和融合。本项目主要成员博士学科方向是计算机体系结构，毕业工作或开展研究后又长期从事云安全、数据安全的实际研发项目和产学研结合，跟本项目研究任务非常契合。

4. 本项目的特色与创新之处；

- **支持标准加密算法和复杂搜索请求的密文搜索技术**

跟绝大多数密文搜索不同，本项目将原来由客户端软件执行的数据加解密和元数据（包括密钥）管理，上位到由访问代理执行，从而达到能支持标准加密算法，跟云服务商透明，且支持复杂搜索请求。当然，在访问代理端须突破敏感数据提取、索引构建、标准加密算法生成的密文数据与元数据映射等新的技术挑战。

- **跨访问代理的数据分享方法**

通过访问代理执行数据加解密和索引构建，带来的代价就是数据分享变得更加困难，密钥安全性更脆弱。这是基于访问代理架构的密文搜索噩待解决但目前缺乏深入研究的问题。本项目拟设计一种双重加密机制，完成密钥的安全交换和分享，从而实现跨访问代理的数据分享。

5. 年度研究计划及预期研究结果（包括拟组织的重要学术交流活动、国际合作与交流计划等）。

5.1 年度研究计划

2019 年 1 月－2019 年 12 月

基于相关工作的研究和实践经验。完成架构的接口设计和详细设计，明确基于访问代理的加密解密流程，完成元数据管理方法与机制的研究。以上述三项研究为理论基础，选定某一典型 SaaS 应用为例，实现原型系统。

2020 年 1 月－2020 年 12 月

在现有原型系统的基础上，实现自动化或半自动化的解析适配云服务协议，标记敏感数据进而进行加解密；实现对多种类型数据的提取和解析；实现标准通用算法的支持和密钥管理技术；研究并实现访问代理的密钥管理与数据映射。

2021 年 1 月－2021 年 12 月

基于已实现的数据保护和密文搜索功能，进一步研究并实现跨访问代理的数据分享技术，设计实现与现代搜索引擎同等水平的各类复杂搜索请求，包括：模糊搜索、含多关键词逻辑的连接搜索、动态搜索等。

2022 年 1 月－2022 年 12 月

对已实现的系统进行性能测试评价，包括建立索引、搜索索引、更新数据、索引存储空间、更新数据所用空间、跨代理分享数据时间等开销代价；研究和分析基于代理的密文搜索体系结构及关键技术的安全性。

5.2 预期研究成果

本课题将从理论和系统两方面入手展开研究工作，预期可以取得如下的研究成果：

- **理论和方法方面**

提出和设计访问代理执行的密文搜索体系架构，深入研究用户数据的自动化提取技术和密钥管理技术。构建多关键字搜索、模糊搜索、动态搜索等高级搜索功能。

- **原型系统方面**

实现与云服务商透明，且支持标准加密算法的密文搜索技术，实现关键技术中指出的云服务协议自动或半自动化解析、密钥管理、高级搜索和数据分享功能。完成既定目标后，进行性能测试和评价。

- **学术论文与专利**

在国际顶级学术会议或ACM IEEE Trans期刊上发表高水平论文10-12 篇，其中SCI检索论文5-6篇，EI检索论文10-12篇；申请国家发明专利2-3项 。

- **人才培养方面**

本课题的开展预期培养博士生3-5名，培养硕士生4-6名。

（二）研究基础与工作条件

1．研究基础（与本项目相关的研究工作积累和已取得的研究工作成绩）；

从2009年即开始云计算与云安全的研究工作：作为核心骨干或子课题负责人完成国家973计划**“信息安全理论及若干关键技术”**，“核高基”国家科技重大专项**“面向新型网络应用模式的网络化操作系统”**，国家高技术研究发展计划(863 计划)项目：**“面向第三方的云平台可信评测技术及系统”**，国家自然科学基金重大研究计划重点支持项目**“可信软件及服务的度量、评估、认证体系研究”**，面上项目**“一种针对云计算环境的安全评估方法”**；主持并完成国家自然科学基金项目：**“云提供商可信性验证与审计研究”**；作为课题负责人完成国家高技术研究发展计划（863计划）项目：**“面向第三方的云平台可信评测技术及系统”**主要负责数据流的审计和脱敏，该工作是本项目申请的研发基础和初步技术思路，也为本项目的研究和学术交流提供了良好环境和人员支持；山东省自主创新及成果转化专项：**“基于监测、取证与追责的虚拟化平台管理系统研发及产业化”**。在此过程中，对云安全的真正痛点、发展方向等形成深刻理解，并积累了本领域坚实的理论和技术基础。

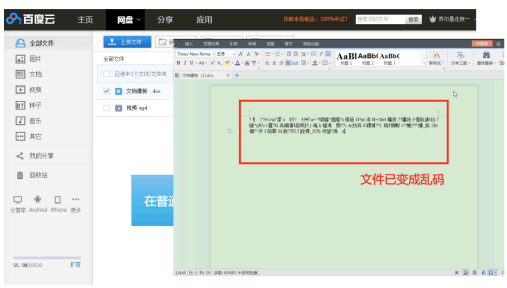
长期致力于：**做有实用价值的创新性研究！**敢于下苦功夫，“真刀真枪”做系统：曾专注3年时间，带领团队对Openstack、Eucalyptus等开源云平台进行彻底解构，并形成国内第一本在源代码层面对云平台进行解构的著作**《拨得云开见日出——解构一个典型的云计算系统》**，能对Openstack、Hadoop等系统做到“指哪打哪，按需定制”。

获得授权中国第一个云存储发明专利：**“一种基于云计算环境的个人数据管理方法**:中国. 专利号：CN101854392A”，以及密文搜索和密文管理专利：**“面向网络化操作系统的可信任虚拟运行平台**，专利号：CN102202046A”，**“一种面向网络化操作系统的可信任在线存储系统**，专利号：CN102413159A”。在申请本项目之前，已培养研究方向为“密文数据搜索和管理”的博士毕业生2名，硕士毕业生4名，在密文搜索领域进行了大量扎实的储备和探索[43][44][45][46][47]。

在上述基础上，本项目清晰确立了针对的问题、预期突破点和创新点，以及初步解

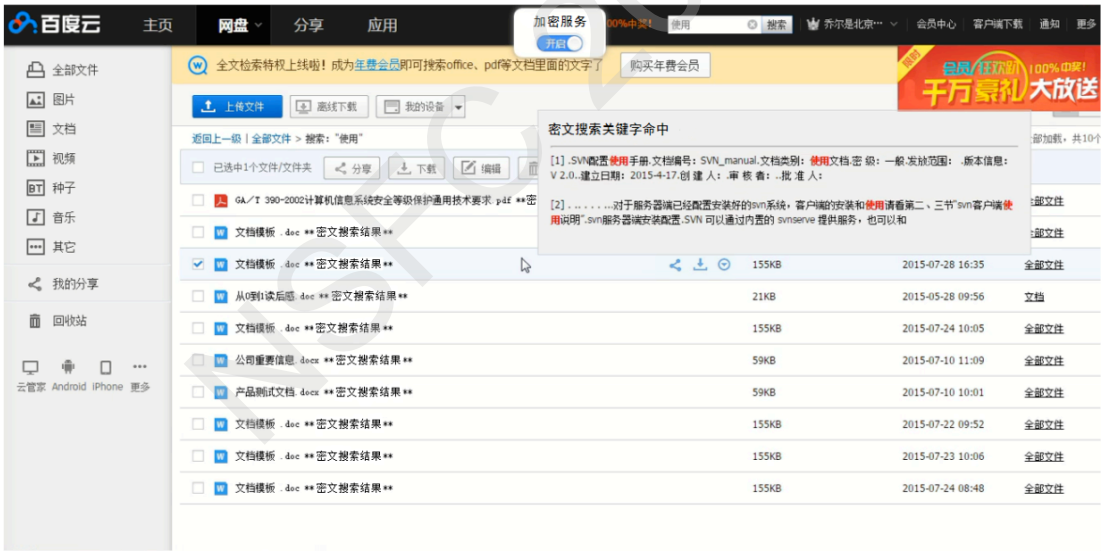
决方案，并已在“拟采取的研究方案及可行性分析”中予以详细说明和分析，在此不再赘述。

更进一步，我们基于本项目设计的研究方案，对一个典型的云服务：百度云盘，初步实现和走通了由访问代理执行的数据加解密和密文全文搜索基本功能。其中若经过访问代理下载或查看文件，访问代理会识别数据流中文件内容，并解密； 若不经过访问代理下载或查看文件，则是密文，如图 6a 所示；由访问代理执行的密文搜索效果如图 6b 所示；用百度网盘自带的搜索功能则搜不到任何密文内容，如图 6c 所示。



a. 百度网盘下载密文文件

b. 百度网盘不经过访问代理的密文搜索效果



c. 百度网盘经过访问代理的密文搜索效果

图 6 百度网盘密文搜索效果图

2. 工作条件（包括已具备的实验条件，尚缺少的实验条件和拟解决的途径，包括利用国家实验室、国家重点实验室和部门重点实验室等研究基地的计划与落实情况）；

本项目依托于哈尔滨工业大学（深圳）计算机科学与技术学院网络空间安全实验室。实验室定位明确，研究方向设置合理，研究内容特色突出，符合学科发展方向，属于科学发展前沿，适应国家重大科技需求。实验室总面积在 3000 平方米左右，拥有总价值

超过 2000 万元的设备仪器，实验室现有院士 1 人、教授近 10 人。现有科研基础、硬件条件和人才队伍等满足实验室建设的基本要求。

在国家和哈尔滨工业大学对网络空间安全领域的大力投入和支持下，实验室拥有各类高性能服务器和刀片集群服务器，以及大型路由器、交换机等各类网络设备；拥有主流的支持分布式计算及服务的软件开发和管理平台；拥有基于面向新型网络应用模式的网络化操作系统的云平台解决方案，能支持大型分布式计算及服务的软件开发支撑条件。

本项目除了拥有身临一线、战斗力强、凝聚力强的实战派科研团队外，我们在跟重庆联通合作建立了支持 Internet 大流量上下行访问的云计算基础设施平台，可供进行实际的云服务数据加解密和密文搜索实验。同时，实验室有各种服务器、PC 50 余台，并相应配有 Windows，Linux，Mac 等环境下的开发平台，供实际测试和终端适配与开发。开展本项目所需的实验条件已基本具备。

3．正在承担的与本项目相关的科研项目情况（申请人和项目组主要参与者正在承担的与本项目相关的科研项目情况，包括国家自然科学基金的项目和国家其他科技计划项目，要注明项目的名称和编号、经费来源、起止年月、与本项目的关系及负责的内容等）；

无

4．完成国家自然科学基金项目情况（对申请人负责的前一个已结题科学基金项目（项目名称及批准号）完成情况、后续研究进展及与本申请项目的关系加以详细说明。另附该已结题项目研究工作总结摘要（限 500 字）和相关成果的详细目录）。

申请人刘川意已完成国家自然科学基金青年科学基金项目《云提供商可信性审计与验证研究》，项目批准号 61202081，目前已结题。

在后续的研究进展中，此项目提出的可信第三方 TTP（Trusted Third Party）云提供商可信性审计和验证模型已经实际应用到典型云平台中；研究与设计的“小云审大云”，已作为国家高技术研究发展计划（863 计划）《面向第三方的云平台可信评测技术及系统》（项目批准号 2015AA016001）的重要技术路线。

《云提供商可信性审计与验证研究》系统性研究了云计算模式的可信问题和主要解决方案，即：对云平台特权操作和行为进行审计和管控；用户自己保护敏感和重要数据，并提出了“数据流脱敏技术”，这正是本次基金申请的重要研究基础和技术思路。本次

项目申请通过实现与云服务商透明、且支持标准加密算法的密文搜索，解决了用户敏感数据难以防护的关键性问题，与前次结题项目相互承接，互为补充。

《云提供商可信性审计与验证研究》项目总结摘要：此项目深度分析了造成云提供商不可信的威胁模型以及典型的云计算平台体系结构，设计了一种新的引入可信第三方 TTP 云提供商可信性审计和验证模型，并针对云平台可信证据收集、云提供商远程可信性验证、云提供商可信审计协议等关键技术进行深入研究。更进一步，为了防止 TTP 成为单点瓶颈或单点故障，通过云计算技术构建 TTP 平台。此项目实现了原型系统，并进行了定量分析、测试和评价，后续研究已将其用于实际云计算平台中。

研究成果目录如下：

[1] **刘川意**, 王国峰, 林杰, 方滨兴. 可信的云计算运行环境构建和审计. 计算机学报, Vol 38(002), pp 286-304, 2016, EI.

[2] 林杰, **刘川意**, 方滨兴. IVirt:基于虚拟机自省的运行环境完整性度量机制. 计算机学报, 38(1), pp 192-203, 2014/8, EI.

[3] Gu Yu, **Liu Chuanyi**, Wang Dongsheng. Fast Recovery and Low Cost Coexist: When Continuous Data Protection Meets the Cloud. IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS, E97D(7), pp 1700-1708, 2014/7, SCI.

[4] 顾瑜, **刘川意**, 鞠大鹏, 汪东升. 基于云存储的块级连续数据保护系统. 计算机科学与探索, 03期, pp 257-265, 2014.

[5] Zhang Xi, **Liu Chuanyi**, Liu Zhenyu, Wang Dongsheng. Improving Cache Partitioning Algorithms for Pseudo-LRU Policies. IEICE Transactions on Information and Systems, E96D(12), pp 2514-2523, 2013/12, SCI.

[6] 项菲, **刘川意**, 方滨兴, 王春露, 钟睿明. 云计算环境下密文搜索算法的研究.通信学报, 07期, pp 143-153, 2013/7/25, EI.

[7] 项菲, **刘川意**, 方滨兴, 王春露, 钟睿明. 新的基于云计算环境的数据容灾策略. 通信学报, 06期, pp 92-101, 2013/6/25, EI.

[8] 王佳慧, **刘川意**, 王国峰, 方滨兴. 基于可验证计算的可信云计算研究. 计算机学报, Vol 38(002), pp 339-350, 2016, EI.

[9] Cui Dong, **Chuan Yi Liu**, Yang Meiqi, Yang Jincui. A Policy-based De-duplication Mechanism for Encrypted Cloud Storage. Journal of Computational Information Systems, 520卷, pp 99-106, 2015/3 3, EI.

[10] Lin Jie, **Chuan Yi Liu**, Ning Zhichun, Fang Binxing. Detecting the run timeattacks in the cloud with an evidence collection based approach. IEEE 3rd International Conference on Cloud Computing and Intelligence Systems, CCIS 2014卷, pp 514-518, 2014, EI.

[11] Lin Jie, **Chuan Yi Liu**, Fang Binxing. TraceVirt: A framework for detecting the non-tampering attacks in the virtual machine. Proceedings of the ACM Conference on Computer and Communications Security, CCS 2014卷, pp 1466-1468, 2014, EI, SCI.

[12] Xiao Da, Yang Lvyin, **Chuan Yi Liu**, Sun Bin, Zheng Shihui. Efficient Data Possession Auditing for Real-World Cloud Storage Environments. IEICE Transactions on Information and Systems, E98D卷, pp 796-806,2014, EI, SCI.

[13] **Chuanyi Liu**, Jie Lin, Binxing Fang. T-YUN: Trustworthiness Verification and Audit on the Cloud Providers. IEICE System, E96D卷, pp 2344-2353, 2013/11, SCI.

[14] **刘川意**, 林杰, 唐博. 面向云计算模式的运行环境可信性动态验证机制. 软件学报, 25(3), pp 662-674, 2013/7/25, EI.

[15] **刘川意**, 方滨兴, 林杰. 基础设施云模块化解构. 北京邮电大学学报, 02期, pp 38-43, 2013/4/15, EI.

[16] Chunlu Wang, **Chuanyi Liu**, Xiaoliang Wang, Yingfei Dong. Effectively Auditing IaaS Cloud Servers. IEEE GLOBECOM, pp 682-688, 2013, EI.

（三）其他需要说明的问题

1. 申请人同年申请不同类型的国家自然科学基金项目情况（列明同年申请的其他项目的项目类型、项目名称信息，并说明与本项目之间的区别与联系）。

无

2. 具有高级专业技术职务（职称）的申请人或者主要参与者是否存在同年申请或者参与申请国家自然科学基金项目的单位不一致的情况；如存在上述情况，列明所涉及人员的姓名，申请或参与申请的其他项目的项目类型、项目名称、单位名称、上述人员在该项目中是申请人还是参与者，并说明单位不一致原因。

无

3. 具有高级专业技术职务（职称）的申请人或者主要参与者是

否存在与正在承担的国家自然科学基金项目的单位不一致的情况；如存在上述情况，列明所涉及人员的姓名，正在承担项目的批准号、项目类型、项目名称、单位名称、起止年月，并说明单位不一致原因。

无

4. 其他。

无

刘川意 简历

哈尔滨工业大学，深圳研究生院，副教授

教育经历（从大学本科开始，按时间倒序排序；请列出攻读研究生学位阶段导师姓名）：

（1）2006.9－2010.1， 清华大学， 计算机科学与技术， 博士， 导师：汪东升

（2）2004.9－2006.7， 清华大学， 计算机科学与技术， 硕士， 导师：汪东升

（3）2000.9－2004.7， 北京交通大学， 计算机科学与信息技术， 学士， 导师：无

科研与学术工作经历（按时间倒序排序；如为在站博士后研究人员或曾进入博士后流动站（或工作站）从事研究，请列出合作导师姓名）：

（1）2016.6-至今，哈尔滨工业大学（深圳校区），计算机学院，副教授

（2）2011.12-2016.6，北京邮电大学，软件学院，副教授

（3）2010.1-2011.12，北京邮电大学，博士后，合作导师：方滨兴

曾使用其他证件信息（申请人应使用唯一身份证件申请项目，曾经使用其他身份证件作为申请人或主要参与者获得过项目资助的，应当在此列明）：

主持或参加科研项目（课题）及人才计划项目情况：

1. 国家重点研发计划项目，多域云安全管控关键技术及系统，2017/07-2020/12，140万元，在研，主持。

2. 威海捷讯通信技术有限公司，基于监测、取证与追责的虚拟化平台安全管理系统研发及产业化，2017/01-2017/12，110万元，在研，主持。

3. 国家科技重大专项，面向网安实验的网络仿真与效果评估关键技术，2016/07-2019/06，600万元，在研，主持。

4. 国家科研发展咨询项目，中国工程院网络空间安全工程科技人才培养规划建议，2016/01-2018/01，60万元，在研，参加。

5. 国家科研发展咨询项目，面向2035的网络舆情管理发展，2016/01-2018/01，73.6万元，在研，参加。

6. 国家高技术研究发展计划（863计划）项目，2015AA016001，基于小云审大云的云平台可信性按需测评与分析技术—面向第三方的云平台可信评测模型及体系结构，2016/01-2017/12，526万元，在研，主持。

7. 国家自然科学基金项目面上项目，61370068，针对云计算环境的安全性分析方法，2014/01-2017/12，73万元，在研，参加。

8. 国家自然科学基金项目青年科学基金项目，61202081，云提供商可信性审计与验证研究，2013/01-2015/12，23万元，已结题，主持。

9. 企、事业单位纵向委托项目（牵头），我国重点领域信息安全保障措施研究，2013/01-2015/12，100万元，已结题，参加。

10. 国家自然科学基金项目重大研究计划重点项目，91118002，可信软件及服务的度量、评估、认证体系标准研究，2012/01-2015/12，300万元，已结题，参加。

代表性研究成果和学术奖励情况（每项均按时间倒序排序）

（请注意：①投稿阶段的论文不要列出；②对期刊论文：应按照论文发表时作者顺序列出全部作者姓名、论文题目、期刊名称、发表年代、卷（期）及起止页码（摘要论文请加以说明）；③对会议论文：应按照论文发表时作者顺序列出全部作者姓名、论文题目、会议名称（或会议论文集名称及起止页码）、会议地址、会议时间；④应在论文作者姓名后注明第一/通讯作者情况：所有共同第一作者均加注上标“#”字样，通讯作者及共同通讯作者均加注上标“*”字样，唯一第一作者且非通讯作者无需加注；⑤所有代表性研究成果和学术奖励中本人姓名加粗显示。）

按照以下顺序列出：①10篇以内代表性论著；②论著之外的代表性研究成果和学术奖励。

一、10篇以内代表性论著

(1) **Chuanyi Liu**(#)(*); Guofeng Wang; Peiyi Han; Hezhong Pan; Binxing Fang, A Cloud Access Security Broker based approach for encrypted data search and sharing, 2017 International Conference on Computing, Networking and Communications (ICNC), 2017.1.26-2017.1.29 **（会议论文）**

(2) **刘川意**(#)(*)；王国峰；林杰；方滨兴，可信的云计算运行环境构建和审计，计算机学报，2016.春，39(02)：286~304 **（期刊论文）**

(3) Guofeng Wang(#); **Chuanyi Liu**(*); Yingfei Dong; Hezhong Pan; Peiyi Han; Binxing Fang, Query Recovery Attacks on Searchable Encryption Based on Partial Knowledge, SecureComm 2017 - 13th EAI International Conference on Security and Privacy in Communication Networks, 2017.10.22-2017.10.25 **（会议论文）**

(4) **Chuanyi Liu**(#)(*); Yu Gu; Linchun Sun; Bin Yan; Dongsheng Wang(*), R-ADMAD: High Reliability Provision for Large-Scale De-duplication Archival Storage Systems, 2009 International Conference on Supercomputing, 2009.6.9-2009.6.11 **（会议论文）**

(5) Peiyi Han(#); **Chuanyi Liu**(*); Binxing Fang; Guofeng Wang; Xiaobao Song; Lei Wan, Revisiting the Practicality of Search on Encrypted Data, Scientific Programming, Scientific Programming, 2016.夏，2016(12) **（期刊论文）**

(6) Guofeng Wang(#); **Chuanyi Liu**(*); Yingfei Dong; Peiyi Han; Hezhong Pan; Binxing Fang, IDCrypt: A Multi-User Searchable Symmetric Encryption Scheme for Cloud Applications, IEEE Access, 2017.12.27, 2017(06): 2908~2921 **(期刊论文)**

(7) 王国峰(#); **刘川意**(*); 潘鹤中; 方滨兴, 云计算模式内部威胁综述, 计算机学报, 2017.春, 40(02): 296~316 **(期刊论文)**

(8) **刘川意**(#)(*); 潘鹤中; 梁露露; 王国峰; 方滨兴, 基于小云审大云的云平台可信评测体系结构与技术研究, 网络与信息安全学报, 2016.春, 10(02): 36~47 **(期刊论文)**

(9) Jie Lin(#); **Chuanyi Liu**(*); Binxing Fang, TraceVirt: A Framework for Detecting the Non-tampering Attacks in the Virtual Machine, Proceedings of the ACM Conference on Computer and Communications Security, 2014.11.3-2014.11.7 **(会议论文)**

(10) **Chuanyi Liu**(#)(*); Xiaojian Liu; Lei Wan, Policy-based de-duplication in secure cloud storage, Communications in Computer & Information Science, 2012.春, 2012(320): 250~262 **(期刊论文)**

二、论著之外的代表性研究成果和学术奖励

(1) **刘川意**(#); 袁玉宇, 拨得云开见日出——解构一个典型的云计算系统, 电子工业出版社, 2012.09.01 **(学术专著)**

(2) 袁玉宇(#); **刘川意**; 郭松柳, 云计算时代的数据中心, 电子工业出版社, 2012.08.01 **(学术专著)**

(3) **刘川意**(#); 韩培义; 王春露; 王国峰; 潘鹤中; 林杰, 基于可信数据格式的通用数据的加密方法、解密 方法及其装置, 2017.07.13, 中国, 201710569667.7 **(专利)**

(4) **刘川意**(#); 潘鹤中; 王春露; 王国峰; 韩培义; 林杰, 一种面向应用的密文搜索方法、装置、代理服务器和系统, 2017.07.18, 中国, 201710586634.3 **(专利)**

(5) **刘川意**(#); 王国峰; 王春露; 潘鹤中; 韩培义; 林杰, 与应用透明的密文搜索方法、网关装置、网关设 备和系统, 2017.07.03, 中国, 201710533383.2 **(专利)**

(6) **刘川意**(#); 王爱兵; 韩培义; 林杰, 一种基于云服务的数据路由方法、装置及系统, 2016.05.25, 中国, 201610006236.5 **(专利)**

(7) **刘川意**(#)；宋小宝；万磊；林杰，一种可信证据的远程验证方法、装置及系统，2016.05.11，中国，201610077855.3 （**专利**）

(8) **刘川意**(#)；袁玉宇；杨金翠；张旸旸；韩强，面向网络化操作系统的可信任虚拟运行平台，2011.3.15，中国，201110061265.9 （**专利**）

(9) 汪东升(#)；**刘川意**，一种基于云计算环境的个人数据管理方法，2010.05.20，中国，201010184346.3 （**专利**）

(10) 袁玉宇(#)；**刘川意**；张旸旸；韩强；杨金翠，一种面向网络化操作系统的可信任在线存储系统，2011.03.15，中国，201110061279.0 （**专利**）

(11) 王奇(#)；张巍；吕先红；曹振奇；汪东升；**刘川意**；鞠大鹏，数据存储方法及设备，2009.12.31，中国，200910216926.3 （**专利**）

(12) 王奇(#)；张巍；吕先红；曹振奇；**刘川意**；鞠大鹏；汪东升，数据存储、读取方法及设备，2009.12.29，中国，200910252582.1 （**专利**）

除非特殊说明，请勿删除或改动简历模板中蓝色字体的标题及相应说明文字

参与者 简历

何慧，哈尔滨工业大学，计算机科学与技术学院，教授。

教育经历（从大学本科开始，按时间倒序排序；请列出攻读研究生学位阶段导师姓名）：

2001/03-2006/10，哈尔滨工业大学，计算机科学与技术学院，博士，导师：胡铭曾

1997/09-1999/07，哈尔滨工业大学，计算机科学与技术学院，硕士，导师：程退安

1993/09-1997/07，哈尔滨工业大学，计算机科学与技术学院，学士

科研与学术工作经历（按时间倒序排序；如为在站博士后研究人员或曾进入博士后流动站（或工作站）从事研究，请列出合作导师姓名）：

2016/12-2018/1，美国加州大学戴维斯分校，计算机学院，访问教授

2016/12-现在，哈尔滨工业大学，计算机科学与技术学院，教授

2015/04-现在，哈尔滨工业大学，计算机科学与技术学院，博士导师

2007/07-2016/12，哈尔滨工业大学，计算机科学与技术学院，副教授

1999/07-2007/06，哈尔滨工业大学，计算机科学与技术学院，讲师

曾使用其他证件信息（申请人应使用唯一身份证件申请项目，曾经使用其他身份证件作为申请人或主要参与者获得过项目资助的，应当在此列明）

无。

主持或参加科研项目（课题）及人才计划项目情况（按时间倒序排序）：

1. 国家自然科学基金面上项目，61472108，基于知识迁移的网络舆论领袖识别方法及其适应性增强研究，2015/01-2018/12，80 万元，在研，主持

2. 国家 863 重点研发项目课题，***关键技术及应用，2011/01-2015/12，1841 万元，已结题，主持

3. 国家重点研发计划-子课题，***检测与发现，2017-2020，86.4 万元，在研，主持

4. 国家部委，***软件开发，2016/09-2017/09，210 万元，已结题，参加

5. 国家部委，***实时综合处理子系统，2016/09-2017/09，610 万元，已结题，参加

6. 网络安全量化评估与趋势预测，国家高技术研究发展计划 863 (2007AA01Z442)，93 万元，2007-2010，已结题，参加

7. 基于异常检测与主动测量的大规模网络协作预警技术，国家高技术研究发展计划 863（2002AA142020），80 万元，2002-2004，已结题，参加

8. 大规模网络安全预警分析技术，信息产业部 242 项目(2005C33)，80 万元，2005-2007，已结题，参加

代表性研究成果和学术奖励情况（每项均按时间倒序排序）

（请注意：①投稿阶段的论文不要列出；②对期刊论文：应按照论文发表时作者顺序列出全部作者姓名、论文题目、期刊名称、发表年代、卷（期）及起止页码（摘要论文请加以说明）；③对会议论文：应按照论文发表时作者顺序列出全部作者姓名、论文题目、会议名称(或会议论文集名称及起止页码)、会议地址、会议时间；④应在论文作者姓名后注明第一/通讯作者情况：所有共同第一作者均加注上标“#”字样，通讯作者及共同通讯作者均加注上标“*”字样，唯一第一作者且非通讯作者无需加注；⑤所有代表性研究成果和学术奖励中本人姓名加粗显示。）

按照以下顺序列出：①10 篇以内代表性论著；②论著之外的代表性研究成果和学术奖励。

一、期刊论文

（1） **何慧**(#)(*); Weizhe Zhang; Chuanyi Liu; Honglei Sun, Trustworthy Enhancement for Cloud Proxy based on Autonomic Computing, IEEE Transactions on Cloud Computing, 2016.11

（2）**何慧**(#)(*); Lijie Cui; Guotao Fan; Dong Wang, Distributed Proxy Cache Technology based on Autonomic Computing in Smart City, Future Generation Computer Systems, 2017.11, 76：370~383, (SCI impact factor 4.787)

（3） **何慧**(#)(*); Dongyan Zhang; Wang xing; Liu Min; Zhangwei Zhe, Guojun Xi, Multi-task Learning-based Security Event Forecast Methods for Wireless Sensor Networks, Journal of Sensors, 2016, 2016(7):1-11, (SCI impact factor 1.14)

（4） **何慧**(#)(*); Zhonghui Du; Weizhe Zhang; Allen Chen, Optimization strategy of Hadoop small file storage for big data in heathcare, The Journal of Supercomputing, 2015.6, 72(10):1-12, (SCI impact factor 1.08)

（5） **何慧**(#)(*); Feng Yana; Zhu Zhenguang; Zhang Weizhe; Cheng Albert, Dynamic Load Balancing Technology for Cloud-oriented CDN, Computer Science Information System, 2015, 12(2):765-786, (SCI impact factor 0.547)

二、会议论文

（1） **何慧(#)(*)**; Hongli Zhang; Lihua Yin; and Yongtan Liu, Topology Awareness on Network Damage Assessment and Control Strategies Generation, In Proceedings of 4th International Conference on Internet Computing for Science and Engineering ICICSE 2009, IEEE Press 2009:169-175, (Ei: 20104413342741)

（2） **何慧(#)(*)**; Hu Mingzeng; Zhang Hongli, Clustering of network link characteristic for detector placement of macroscopical prewarning, First International Multi- Symposiums on Computer and Computational Sciences IMSCCS'06, 2006, (2):155-159, (Ei:20065110322777)

（3） **何慧(#)(*)**; Zhang Hongli; Zhang Weizhe; Hu Mingzeng; Tang Zhenjiang, Early Warning of Active Worms based on Multi-Similarity, In: Proc of the 4th International Conference on Machine Learning and Cybernetics (ICMLC 2005), Guangzhou China, 2005.8.18-2005.8.21, IEEE Press pp:3876~3883

（4） **何慧(#)(*)**; Hu Mingzeng; Zhang Weizhe; Zhang Hongli; Yang Zhi, Topology-based Macroscopical Response and Control Technology for Network Security Event, Computational Intelligence and Security, Springer Berlin Heidelberg, 2005:560-566. (EI: Compendex: 06229909405 SCI&ISTP IDS Number: BDQ20)

（5） **何慧(#)(*)**; Mingzeng Hu; Hongli Zhang; Zhenjiang Tang, On the Effectiveness of multi-similarity for early detection of worms, International Conference on Parallel and Distributed Computing, Dalian China, 2005.12.5-2005.12.8, IEEE Press 2005 229-233

三、专著

（1） **何慧(#)**; 史建焘; 季振洲; 陈立章. 《网络安全实验培训教程》（国家网信办培训教材），人民邮电出版社, 560 千字, 2017.1

（2） 吕德生(#); **何慧**; 梁冰.《基于数字仿真模型的网络舆论引导理论与应用》. 科学出版社.2015.3

四、授权发明专利

（1） **何慧(#)**; 张伟哲; 余翔湛; 张宏莉; 叶麟; 詹东阳等, 云平台vmm层行为监控方法, 2018.01.08, 中国, 201510096203.X

（2） **何慧(#)**; 张伟哲; 詹东阳; 李琛轩等, 一种面向Xen虚拟化平台的隐藏方法, 2017.06.20,中国, 201510096205.9

（3） **何慧(#)**; 张伟哲; 张宏莉; 李乔; 张永胜; 秦泓洋; 王冬; 范国涛, 可控分布

式代理平台, 2015.10.28, 中国, CN201310157321.8

（4） **何慧(#)**; 李乔; 张伟哲; 刘亚维; 王健; 王冬, 基于访问密度的Web缓存替换方法, 2016.04.04, 中国, CN201310054554.5

（5） **何慧(#)**; 张伟哲; 李乔; 张宏莉; 王雅山; 范国涛; 秦泓洋, 基于信任的网络群体异常感知方法, 2017.03.22, 中国, CN201310336960.0

（6） **何慧(#)**; 张伟哲; 李乔; 王冬; 王健; 范国涛; 秦泓洋, 基于自主计算的代理缓存集群异常检测系统, 2016.06.24, 中国, CN201310441398.8

（7） **何慧(#)**; 张伟哲; 张宏莉; 杨志; 王星; 杨贤青, 基于MLkP/CR算法的无向图分割方法, 2012.04.18, 中国, CN200910073338.9

（8） **何慧(#)**; 张宏莉; 王星; 杨贤青; 马红梅; 陈益坚, 一种基于网络拓扑特征的网络安全量化评估方法, 2012.04.18, 中国, CN2010101084203

（9） **何慧(#)**; 张宏莉; 杨志; 吴华; 王星; 王耀, 网络安全事件可视化系统, 2012.10.10, 中国, CN2010 10109333.X

（10）张宏莉(#); **何慧**; 张伟哲; 田志宏; 杨志; 杨天龙, 基于矢量图和位图的大规模网络拓扑平面可视化方法, 2011.12.07, 中国, CN200910310286.2

（11） 张宏莉(#); **何慧**; 王星; 杨贤青; 许刚; 刘静; 李文娟; 胡卫国, 一种大规模安全事件模拟与仿真方法及控制方法, 2012.09.26, 中国, CN201010109449.3

除非特殊说明，请勿删除或改动简历模板中蓝色字体的标题及相应说明文字

参与者 简历

林杰，哈尔滨工业大学（深圳），计算机科学与技术学院，博士后

教育经历（从大学本科开始，按时间倒序排序；请列出攻读研究生学位阶段导师姓名）：

2011/09-2015/10，北京邮电大学，计算机学院，博士，方滨兴

2009/09-2011/06，云南财经大学，信息学院，硕士，余建坤

2005/09-2009/06，集美大学，计算机工程学院，学士

科研与学术工作经历（按时间倒序排序；如为在站博士后研究人员或曾进入博士后流动站（或工作站）从事研究，请列出合作导师姓名）：

2017/03-至今，哈尔滨工业大学（深圳），计算机科学与技术学院，博士后，合作导师：方滨兴

曾使用其他证件信息（申请人应使用唯一身份证件申请项目，曾经使用其他身份证件作为申请人或主要参与者获得过项目资助的，应当在此列明）

无。

主持或参加科研项目（课题）及人才计划项目情况（按时间倒序排序）：

1. 国家高技术研究发展计划(863 计划)项目，2015AA016001，面向第三方的云平台可信评测技术及系统，2016/01-2017/12，526万元，在研，参加

2. 国家自然科学基金，61370068，针对云计算环境的安全性分析方法，2014/01-2017/12，73万元，已结题，参加

3. 国家自然科学基金，61202081，云提供商可信性审计与验证研究，2013/01-2015/12，23万元，已结题，参加

4. 国家自然科学基金，91118002，可信软件及服务的度量、评估、认证体系标准研究，2013/01-2015/12，23万元，已结题，参加

5. 国家高技术研究发展计划(863 计划)项目，2012AA01A404，基于eID的典型示范应用，2012/06-2014/12，1500万元，已结题，参加

代表性研究成果和学术奖励情况（每项均按时间倒序排序）

（请注意：①投稿阶段的论文不要列出；②对期刊论文：应按照论文发表时作者顺序列出全部作者姓名、论文题目、期刊名称、发表年代、卷（期）及起止页码（摘要论文请加以说明）；③对会议论文：应按照论文发表时作者顺序列出全部作者姓名、论

文题目、会议名称(或会议论文集名称及起止页码)、会议地址、会议时间；④应在论文作者姓名后注明第一/通讯作者情况：所有共同第一作者均加注上标“#”字样，通讯作者及共同通讯作者均加注上标“*”字样，唯一第一作者且非通讯作者无需加注；⑤所有代表性研究成果和学术奖励中本人姓名加粗显示。）

按照以下顺序列出：①10篇以内代表性论著；②论著之外的代表性研究成果和学术奖励。

一、期刊论文

(1) **林杰**(#); 刘川意(*); 方滨兴, IVirt：基于虚拟机自省的运行环境完整性度量机制[J], 计算机学报, 2015 38(1): 191-203, （EI检索：20150600487762）

(2) Liu C(#)(*); **Lin J**; Fang B, T-yun: Trustworthiness verification and audit on the cloud providers [J], IEICE Transactions on Information and Systems, 2013 E96-D(11): 2344-2353, （SCI检索：WOS:000327168600005, EI检索：20134917055176）

(3) 刘川意(#)(*); **林杰** ; 唐博, 面向云计算模式运行环境可信性动态验证机制[J]. 软件学报, 2014 25(3): 662-674, （EI检索：20141317523629）

(4) 刘川意(#)(*); 方滨兴; **林杰**, 基础设施云模块化解构[J], 北京邮电大学学报, 2013 36(2): 38-43, （EI检索：20132516433020）

(5) Liu C(#)(*); Wang Y; **Lin J**, A Policy-based De-duplication Mechanism for Encrypted Cloud Storage [J], Journal of Computational Information Systems, 2014 10(6): 2297-2304, （EI检索：20142117743780）

(6) 刘川意(#)(*); **林杰**, 一种基础设施云系统——YUN系统[J], 中兴通讯技术, 2012 18(6): 26-29

(7) 刘川意(#)(*); 王国峰; **林杰**; 方滨兴, 可信的云计算运行环境构建和审计[J]. 计算机学报, 2016 39(2): 339-350, （EI检索：20161102091776）

二、会议论文

（1） **Lin J**(#); Liu C(*); Fang B, TraceVirt: A Framework for Detecting the Non-tampering Attacks in the Virtual Machine, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York: ACM Press 2014: 1466-1468, （EI检索：20144700229768）

（2） **Lin J**(#); Liu C(*); Ning Z, Detecting The Run Time Attacks In The Cloud With An Evidence Collection Based Approach, Proceedings of the CCIS2014, IEEE 2014: 514-518

（3） Wang G(#); Liu C(*); **Lin J**, Transparency and Semantics Coexist: When Malware

Analysis Meets the Hardware Assisted Virtualization, Proceedings of the ISCTCS 2013, Springer-Verlag Berlin Heidelberg, 2014: 29-37, （EI检索：20143118006724）

三、专著

无

四、授权发明专利

（1） 刘川意(#)；宋小宝；万磊；**林杰**，一种可信证据的远程验证方法、装置及系统，2016.10.19，中国，201610077855.3

（2） 刘川意(#)；王爱兵；韩培义；**林杰**，一种基于云服务的数据路由方法、装置及系统，2016.10.06，中国，201610006236.5

附件信息

序号	附件名称	备注	附件类型
1	论文1	A Cloud Access Security Broker Based Approach for Encrypted Data Search and Sharing	代表性论著
2	论文2(第一部分)	可信的云计算运行环境构建和审计（1）	代表性论著
3	论文2(第二部分)	可信的云计算运行环境构建和审计（2）	代表性论著
4	论文3	Query Recovery Attacks on Searchable Encryption Based on Partial Knowledge	代表性论著
5	论文4	R-ADMAD High Reliability Provision for Large-Scale De-duplication Archival Storage Systems	代表性论著
6	论文5	Revisit the Searchable Data Encryption from Cloud Access Broker ‘s perspective	代表性论著

签字和盖章页(此页自动生成,打印后签字盖章)

接收编号：6187060411

申 请 人： 刘川意 依托单位： 哈尔滨工业大学

项目名称： 基于访问代理体系结构的密文搜索关键技术研究

资助类别： 面上项目 亚类说明：

附注说明：

申请人承诺：

我保证申请书内容的真实性。如果获得资助，我将履行项目负责人职责，严格遵守国家自然科学基金委员会的有关规定，切实保证研究工作时间，认真开展工作，按时报送有关材料。若填报失实和违反规定，本人将承担全部责任。

签字：

项目组主要成员承诺：

我保证有关申报内容的真实性。如果获得资助，我将严格遵守国家自然科学基金委员会的有关规定，切实保证研究工作时间，加强合作、信息资源共享，认真开展工作，及时向项目负责人报送有关材料。若个人信息失实、执行项目中违反规定，本人将承担相关责任。

编号	姓名	工作单位名称 （应与加盖公章一致）	证件号码	每年工作 时间（月）	签字
1	何慧	哈尔滨工业大学	220202197404202124	8	
2	林杰	哈尔滨工业大学	350881198702110035	8	
3	段少明	哈尔滨工业大学	43052519940216491X	8	
4	冯宽	哈尔滨工业大学	41272819951117287X	8	
5	赵艺茗	哈尔滨工业大学	321324199503260036	8	
6	郑旭如	哈尔滨工业大学	440823199310277357	8	
7	庄荣飞	哈尔滨工业大学	350502199206231519	8	
8					
9					

依托单位及合作研究单位承诺：

已按填报说明对申请人的资格和申请书内容进行了审核。申请项目如获资助，我单位保证对研究计划实施所需要的人力、物力和工作时间等条件给予保障，严格遵守国家自然科学基金委员会有关规定，督促项目负责人和项目组成员以及本单位项目管理部门按照国家自然科学基金委员会的规定及时报送有关材料。

依托单位公章	合作研究单位公章1	合作研究单位公章2
日期：	日期：	日期：