大数据统一管理与智能推演支撑平台分系统软件-招标需求公示

各潜在供应商：

依照《深圳经济特区政府采购条例》相关规定，我公司计划对大数据统一管理与智能推演支撑平台分系统软件项目进行公开招标，现将有关情况向潜在供应商公示，征求意见：

1.采购人名称：鹏城实验室

2.采购项目名称：大数据统一管理与智能推演支撑平台分系统软件

3.采购项目描述：(内容、用途、数量、简要技术需求等)：详见附件链接。

4.采购方式：公开招标

5.评审标准：综合评标，详见附件链接。

6.征求意见期限：从2019年11月26日起至2019年11月28日止

7.招标代理机构：

联系人：吴小姐 陈先生

地址：深圳市福田区天安数码城创新科技广场一期B座408B室

联系电话：0755-83232102　88602731

办公邮箱：szrnxzb@163.com

8.备注：潜在供应商对公示内容有异议的，请于公示之日内以实名书面（包括联系人、地址、联系电话）形式（加盖公章）将意见反馈至深圳市瑞凝信招标咨询有限公司办公邮箱。

深圳市瑞凝信招标咨询有限公司

2019年11月25日

第一部分　投标人资格要求

符合《政府采购法》第二十二条规定的供应商条件并同时满足以下要求：

（1）具有独立法人资格或具有独立承担民事责任的能力的其它组织（提供营业执照或事业单位法人证等法人证明扫描件，原件备查）；

（2）参与本项目投标前三年内，在经营活动中没有重大违法记录（由供应商在《投标人具备投标资格的证明文件》中作出声明）；

（3）参与本项目政府采购活动时不存在被有关部门禁止参与政府采购活动且在有效期内的情况（由供应商在《投标人具备投标资格的证明文件》中作出声明）；

（4）参与政府采购项目投标的供应商未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单（由供应商在《投标人具备投标资格的证明文件》中作出声明）。

（5）本项目不接受联合体投标，不得分包、转包；

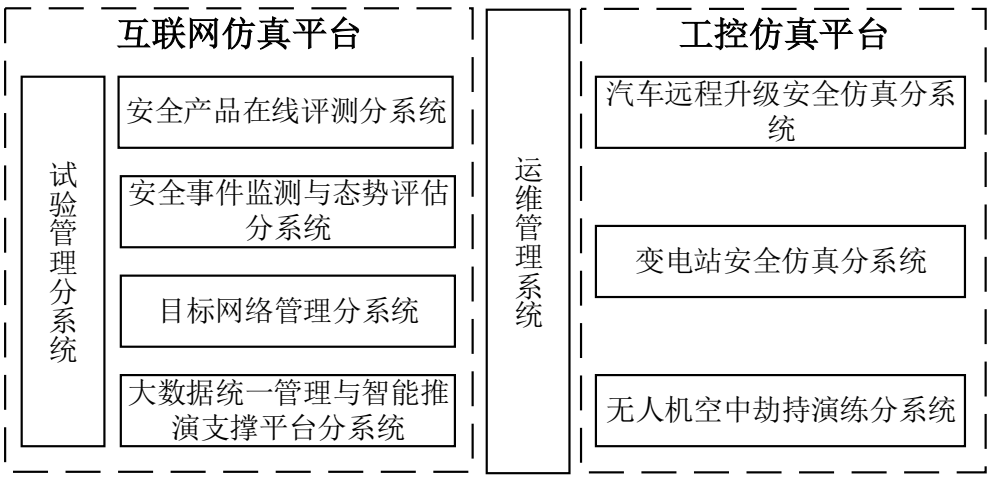
第二部分 项目基本情况

序号	服务分项名称	单位	数量	项目预算	备注
1	大数据统一管理与智能推演支撑平台分系统软件	套	1	1650 万元	
合计（单位：元）:16,500,000.00					

第三部分、需求内容表述

3.1 招标项目概况

大数据统一管理与智能推演支撑平台分系统是网络技术仿真验证平台的重要组成部分。网络仿真平台由互联网仿真平台、工控安全仿真平台、运维管理系统三部分组成，其中互联网仿真平台包括试验管理、目标网络、安全事件监测与态势评估、大数据统一管理与智能推演支撑平台、在线评测平台等五个分系统，工控安全仿真平台包括汽车远程升级安全仿真、变电站安全仿真、无人机空中劫持演练等三个分系统。



大数据统一管理与智能推演支撑平台分系统为网络仿真平台的多模态数据提供数据加载、清洗、存储、管理、统一查询和分布式计算平台，实现高吞吐量、高并发的数据访存；为网络安全知识的表示、构建、管理、利用提供开发框架、基础组件和运行环境，并为数据流上的关联分析提供在线高性能计算平台。

3.2 项目管理要求

1）中标方需在中标后两周内提交《软件开发计划书》；

2）项目实施过程中，中标方需服从招标方项目管理；

3）针对定制需求的开发，中标方必须派人驻场进行开发和测试。

3.3 项目技术及人员要求

3.3.1 技术要求

本项目是组成网络技术仿真验证平台（第二阶段）的一个软件分系统，该软件的结构必须符合需求规范中的分系统、子系统、模块 3 层结构分解要求，以及各层次对应的分系统、子系统、模块的功能和性能指标要求。本项目的需求规范参见附件一。

3.3.2 人员要求

项目负责人和项目参研人员明确，参研技术人员 30 人以上。项目负责人及参研人员需全职参与项目研发。项目负责人具有计算机专业硕士以上学历，在投标人企业工作两年以上，具有大数据方面的三年以上的工作经验。项目实施与服务期间，参研人员变更比例不超过 30%。

3.4 项目清单

本项目采购内容为软件定制开发，内容为：大数据统一管理与智能推演支撑平台分系统软件；数量为：1 套。

本采购的交付物至少应包括：软件的目标代码、源代码、自测测试的目标代码、源代码，以及针对所采购产品的需求规格说明书、概要设计说明书、详细设计说明书、自测测试方案、自测测试报告、产品说明书、安装与使用手册等文档资料。交付物形式：包含全部交付内容的光盘 4 套。

3.5 质量考核验收标准及违约金

质量考核验收标准：全部合同指标通过具有 CNAS 资质且获招标方认可的第三方测试；组织专家进行验收评审，并在评审中获通过。

违约金：合同款的 30%。

3.6 保修或售后服务要求

1）中标方需提供 7X24 小时电话服务；

2）软件运行期间如果出现问题，且非现场服务 24 小时内无法解决问题，中标方须在 24 小时内赶赴现场排查问题，直至问题解决；

3）提供原厂 3 年免费维保服务，在维护期内，必须派至少 1 人驻场维护；购买的各种软件为鹏城实验室提供永久授权；不限制安装次数；

4）在质保期内提供不少于 3 次的免费系统使用培训或开发培训。

3.7 服务期限

自合同签署生效后一年。

3.8 付款方式

合同正式生效后，支付合同总额 50%的价款，所有交付物通过具有 CNAS 资质且获招标方认可的第三方测试后支付合同总额 30%的价款，所有交付物通过验收后支付合同总额 20%的价款。

3.9 投标报价要求

1)本项目服务费采用包干制，应包括服务成本、法定税费和企业的利润。由企业根据招标文件所提供的资料自行测算投标报价；一经中标，投标报价总价作为中标单位与采购单位签定的合同金额，合同期限内不做调整；

2)投标人应根据本企业的成本自行决定报价。不得以低于成本的报价竞标；评标委员会认为投标人的报价明显低于其他通过符合性审查投保人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料，投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

3)投标人的投标报价不得超过财政预算限额或最高投标限价；

4)投标人的投标报价，应是本项目招标范围和招标文件及合同条款上所列的各项内容中所述的全部，不得以任何理由予以重复，并以投标人在投标文件中提出的综合单价或总价为依据；

5)除采购代理机构通过修改招标文件予以更正，否则，投标人应毫无例外地按招标文件所列的清单中项目和数量填报综合单价和合价。投标人未填综合单价或合价的项目，在实施后，视作该项费用已包括在其它有价款的综合单价或合价内，不得申请额外支付；

6)投标人应先到项目地点踏勘以充分了解项目的位置、情况、道路及任何其它足以影响投标报价的情况，任何因忽视或误解项目情况而导致的索赔或服务期限延长申请将不获批准；

7)投标人不得期望通过索赔等方式获取补偿，否则，除可能遭到拒绝外，还可能将被作为不良行为记录在案，并可能影响其以后参加政府采购的项目投标。各投标人在投标报价时，应充分考虑投标报价的风险。

3.10 注意事项

1）中标人不得将项目非法分包或转包给任何单位和个人。否则，采购单位有权即刻终止合同，并要求中标人赔偿相应损失。

2)投标人若认为招标文件的技术要求或其他要求有倾向性或不公正性，可在招标答疑阶段提出，答疑阶段未提出，则默认投标人已接受本项目招标文件的所有条款，开标后不得提出对招标条款的质疑，以维护招标行为的公平、公正。

3)投标人使用的标准必须是国际公认或国家、或地方政府颁布的同等或更高的标准，如投标人使用的标准低于上述标准,评标委员会将有权不予接受，投标人必须列表将明显的差异详细说明。

4)为此项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加此项目的其他招标采购活动。投标方需提供承诺函。

第四部分、评标信息

类别	评分项目	权重	评分标准
	指标响应情况	16	评审内容： 投标文件应对招标文件的功能指标和性能指标给出响应偏离表，标记为“★”的指标是关键技术条款，正偏离不加分，如不满足其投标予以拒绝；对标“▲”的指标，若响应为负偏离，则扣 4 分；其余负偏离，每一项扣 2 分。负偏离项超过 8 项则废标。无负偏离，该项得满分。 标▲需提供官网截图等证明材料，否则默认为负偏离 标★需提供官网截图等证明材料，否则默认为负偏离
	项目重点难点分析和应对的技术路线	7	评审内容： 能否全面、准确地识别项目的重难点问题，并清晰地加以阐述和分析，拟采用的技术路线与解决方法的先进性与可行性。 根据招标文件的需求和投标文件响应情况进行横向比较，分档评分：评价为优得 7 分；评价为良得 5 分；评价为中得 2 分；评价为差不得分。评价为“差”的，专家需说明情况。
	质量（完成时间、进度控制）保障措施及方案	3	评审内容： 进度安排是否合理，能否满足项目要求，能否提供有效的质量保障措施。评价为优得 3 分；评价为良得 2 分；评价为中得 1 分；评价为差不得分。评价为“差”的，专家需说明情况。
	项目实施与质保期间的驻场开发、培训、运维等服务承诺	3	评审内容： 投标文件的项目实施计划关于项目建设（开发测试）与质保（上线运维）期间，承诺的驻场计划、项目组成员稳定性及其他培训与服务内容。其中，开发测试期间（合同签订至项目验收期间）驻场人数不少于 30 人，少于 30 人不得分，达到 30 人以上再根据招标文件的需求和投标文件响应情况进行横向比较，分档评分：评价为优得 3 分；评价为良得 2 分；评价为中得 1 分；评价为差不得分。评价为“差”的，专家需说明情况。
	违约承诺	1	评审内容： 具有明确的违约承诺，保证措施合理有针对性。 评价为合格得 1 分，不合格不得分。
	研发方案总体评价	10	评审内容： 1、对项目背景是否能全面、准确的了解； 2、项目实施思路是否清晰，技术路线是否完整、正确； 3、项目实施内容是否全面，合理、深入，符合本次采购需求。 根据招标文件的需求和投标文件响应情况进行横向比较，分档评分：评价为优得 10 分；评价为良得 6 分；评价为中得 3 分；评价为差不得分。评价为“差”的，专家需说明情况。
价格标 S）（总分 40 分）	投标总价	40	得分按以下公式计算：得分=Z/Sn×40 其中：Z--通过资格性审查和符合性审查且报价不超过预算控制金额的最低评标报价。 Sn--通过资格性审查和符合性审查且报价不超过预算控制金额的评标报价。 根据财政部、工业和信息化部关于《政府采购促进中小企业发展暂行办法》第五条的规定，评委按照投标人提供的《中小企业声明函》中的相

			关内容，对同时符合以下条件的投标价格给予6%的扣除，扣除后的价格作为投标人的评审报价进行价格评比： ① 投标人为小型或微型企业； ② 所投全部投标产品、承担的项目全部工程或者全部服务均由小型或微型企业制造或提供。 评标价计算公式：若投标人适用《政府采购促进中小企业发展暂行办法》：投标人评标报价=投标报价*（1－6%）若投标人不适用《政府采购促进中小企业发展暂行办法》：投标人评标报价=投标报价
商务标（X）（总分20分）	企业资质（3分）	1	具有由CMMI研究院授权的评估机构颁发的软件产品质量成熟度CMMI认证证书，CMMI5及以上得1分，CMMI4得0.5分。 注：提供证书复印件加盖投标人公章。
		0.5	具有由国家认证认可监督管理部门批准设立的认证机构颁发的ISO20000信息技术服务管理体系认证证书得0.5分。 注：提供证书复印件加盖投标人公章。
		0.5	具有由国家认证认可监督管理部门批准设立的认证机构颁发的ISO27001信息安全管理体系认证证书得0.5分。 注：提供证书复印件加盖投标人公章。
		0.5	具有由国家认证认可监督管理部门批准设立的认证机构颁发的企业知识产权管理体系认证证书得0.5分。 注：提供证书复印件加盖投标人公章。
		0.5	具有由国家认证认可监督管理部门批准设立的认证机构颁发的ISO9001质量管理体系认证证书得0.5分。 注：提供证书复印件加盖投标人公章。
	业绩和经验	3	近3年以来（2016年1月至今，以签订合同时间为准），具有政府大数据信息化软件类或高速数据流处理软件类项目建设经验，每提供一个已验收项目合同得1分，最多3分。 注：需提供合同关键页和加盖公章的验收报告的复印件作为证明材料，并在复印件上加盖投标人公章。
	拟投入本项目的团队人员情况	1	拟派项目组成员（除项目经理外）资质要求： 1）具有不少于1名持有人社部门或人力资源开发部门颁发的《系统架构设计师》或《系统分析师》或《系统规划与管理师》证书之一，得0.5分。 2）具有不少于1名持有人社部门或人力资源开发部门颁发的《数据库系统工程师》或《软件设计师》或《信息技术支持工程师》或《高级软件工程师》证书之一，得0.5分。 注：同一人员拥有多个证书，只按一个证书计分，不重复计分，提供人员资质证书及近三个月投标人为其购买的社保证明复印件，并加盖投标人公章。
	软件成熟度	5	具有数据接入平台、数据处理引擎、数据组织管理平台、数据治理平台或服务资源目录管理平台等相关的软件著作权登记证书，且获得软件著作权的时间早于招标公告发布时间。每个得1分，满分5分。 注：提供证书复印件加盖投标人公章。
	投标人自主	3	具有海量数据或流数据处理方面的授权发明专利，每项1分，满分3分。

	知识产权产品（发明专利）情况		注：提供证书复印件加盖投标人公章。
	诚信评价	5	根据《深圳市财政委员会关于印发〈深圳市政府采购供应商诚信管理暂行办法操作细则〉的通知》（深财购[2017]42 号）的要求，投标人在参与政府采购活动中存在诚信相关问题且在主管部门相关处理措施实施期限内的，本项不得分，否则得满分。投标人无需提供任何证明材料，由工作人员向评审委员会提供相关信息。
评标总得分（N） 总分 100 分		N=J+S+X	

第五部分、大数据统一管理与智能推演支撑平台分系统技术需求

1. 分系统概述

大数据统一管理与智能推演支撑平台分系统为网络仿真验证平台的结构化、半结构化和非结构化等多模态数据提供数据加载、清洗、存储、管理、查询和分布式计算平台，实现高吞吐量、高并发的数据访存，并面向各上层业务分系统的数据生产和使用特点，定制一组高性能、便捷的统一接口；另一方面，为网络安全知识的表示、构建、管理和利用提供开发框架、基础组件和运行环境，为流数据上的知识关联分析提供高性能流计算环境。

2. 分系统组成

大数据统一管理与智能推演支撑平台分系统由多元网络安全知识库和多模态网络仿真数据库子系统组成，如图 1 所示。

多元网络安全知识库为网络安全知识和试验场景知识提供统一的知识表达，负责管理知识子图库，并提供知识抽取与智能推演的计算环境，为每次试验构建试验场景知识，提供基于试验场景知识模板的高性能流数据分析。

多模态网络仿真数据库子系统负责加载、清洗、存储、管理整个网络仿真平台的多模态数据，并提供高性能数据查询和数据分析工具。

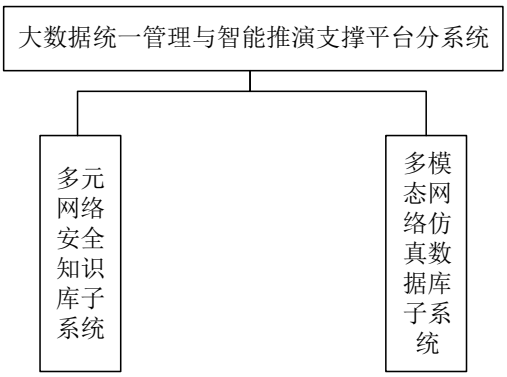


图 1 大数据统一管理与智能推演支撑平台分系统组成图

3. 分系统控制与数据流图

该分系统的两个子系统与外部分系统的交互关系如下图 2、图 3、图 4 所示。

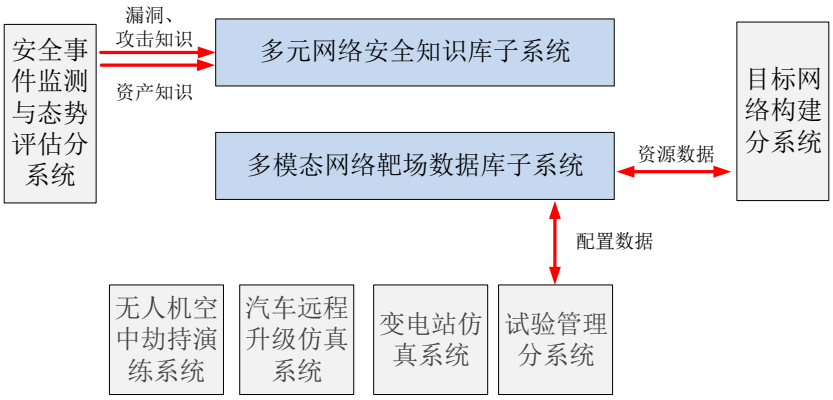


图 2 大数据统一管理与智能推演支撑平台分系统（试前信息交互）

如图 2 所示，在试验开始前，由安全事件监测与态势评估分系统向多元网络安全知识库输入各类网络安全攻击知识，以及网络仿真平台的各类软硬件资产实例信息，由安全事件监测与态势评估分系统在多元网络安全知识库里构建知识子图库和试验场景知识图谱。另外一方面，试验管理分系统根据用户对试验的配置，将相关配置信息存储到多模态网络仿真数据库子系统中，并支持目标网络管理分系统从多模态网络仿真数据库子系统中加载各类资源数据，用于构建目标网络环境。

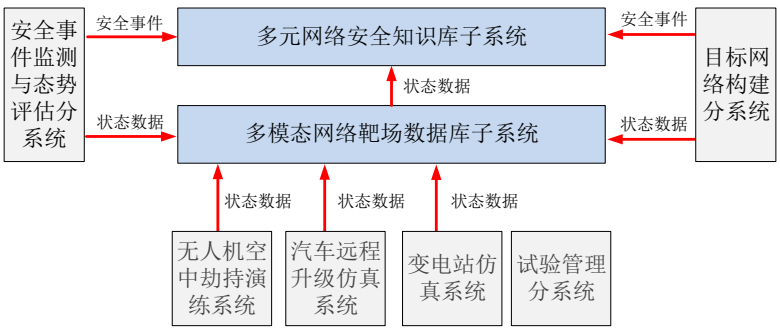


图 3 大数据统一管理与智能推演支撑平台分系统（试中信息交互）

如图 3 所示，试验运行过程中，安全事件监测与态势评估分系统、目标网络管理分系统负责监

测网络仿真平台运行状态，将采集到的安全事件推送给多元网络安全知识库。同时，这两个分系统，以及无人机空中劫持演练分系统、汽车远程升级安全仿真分系统、变电站安全仿真分系统，在试验运行过程中，会将网络流量以及各类探针采集到的状态数据，发送到多模态网络仿真数据库子系统中。多模态网络仿真数据库子系统对高速到达的多模态运行数据进行清洗融合后，及时、可靠地存储到数据库中，并根据多元网络安全知识库的订阅要求，推送清洗后的状态数据。多元网络安全知识库在安全事件监测与态势评估分系统的管理下，基于试验前构建好的试验场景知识图谱，对高速到达的数据流进行在线分析。

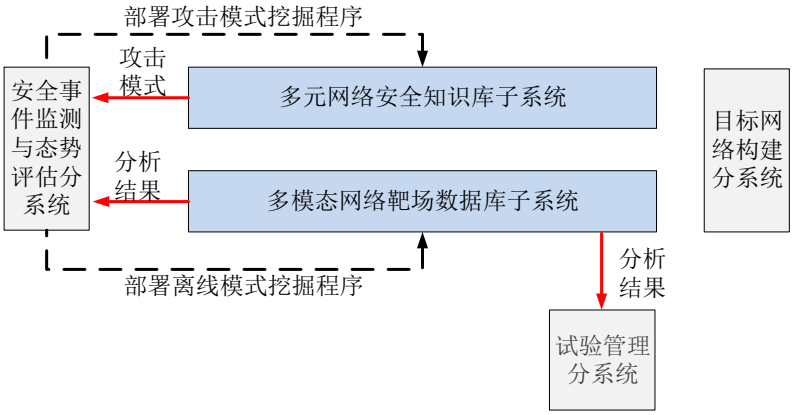


图 4 大数据统一管理与智能推演支撑平台分系统（试后信息交互）

如图 4 所示，试验结束后，为安全事件监测与态势评估分系统在多元网络安全知识库中部署模式挖掘程序，支持其进行推演分析，发现新的攻击模式。同时，为安全事件监测与态势评估分系统还在多模态网络仿真数据库子系统中部署离线挖掘程序，支持其对各类运行过程数据进行统计分析和关联挖掘，获得分析结果。此外，试验管理分系统也将调用相关在线查询和分析接口，从多模态网络仿真数据库子系统中获取回放数据和在线交互式分析结果。

4. 分系统总体要求

大数据统一管理与智能推演支撑平台分系统为网络仿真平台提供统一的数据管理服务和智能分析计算环境。主要功能要求包括：

1. 网络安全知识管理方面，支持网络安全知识中多元实体的复杂关联关系表示，提供网络安全知识和试验知识的存储、索引、删除、修改、查询等管理服务；

2. 网络安全知识推演分析方面，提供网络安全知识和试验知识构建与推演计算平台，提供流数据的在线知识匹配与关联分析平台；

3. 网络仿真数据管理方面，支持网络仿真平台环境中的各类结构化流数据和非结构化文件数据的高效存储与管理；

4. 网络仿真数据分析计算方面，提供多模态试验数据挖掘分析的分布式计算环境，提供网络

仿真平台试验流数据清洗与融合的映射框架。

关键性能指标包括：

1. 规模方面，支持 PB 级网络仿真平台数据和亿级规模网络安全知识的存储管理与分布式计算；

2. 并发性方面，支持 1000 个试验同时运行，可对同时运行的试验提供在线关联分析、配置数据加载与查询、状态数据入库与索引；

3. 速度方面，面向业务分系统需求的数据与知识查询平均响应延迟小于 100ms，数据总体存储加载速率不小于 100MB/s。

5. 多元网络安全知识库子系统

5.1 子系统概述

多元网络安全知识库为知识子图库的表示、获取、构建、存储、管理和利用提供平台支撑。在试验运行过程中，提供试验场景知识图谱与安全事件和各类状态数据的高性能匹配计算环境。此外，为网络仿真平台提供知识推演的分布式计算平台。

5.2 子系统组成

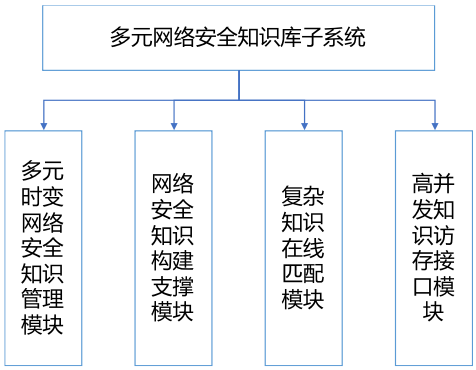


图 5 多元网络安全知识库组成图

多元网络安全知识库由多元时变网络安全知识图谱管理模块、高并发知识访存接口、网络安全知识构建支撑模块、复杂知识在线匹配模块组成。高并发知识访存接口可在线分解与融合多个物理知识库的查询与入库请求，并提供主流的 Gremlin 图查询语言接口和便于开发的 Restful 编程接口。网络安全知识构建支撑模块针对网络安全知识图谱的数据特点，内置网络安全知识对象的数据模型，为知识抽取与推演程序提供快速开发框架和分布式计算环境，并提供一组知识抽取和推演计算的基础组件。复杂知识在线匹配模块基于实时流立方技术实现，能够实时分析各类安全设备的探测结果数据流，并将处理后的中间结果合并生成一个多维度的可计算数据立方，支持网络仿真平台安全事件数据和状态数据的实时攻击检测。

5.3 子系统控制与数据流图

该子系统的数据交互与控制逻辑如图 6、图 7、图 8 所示。

在试前准备阶段，安全事件监测与态势评估分系统负责向本子系统的知识构建支撑模块中写入安全知识基础数据。网络安全知识构建支撑模块在安全事件监测与态势评估分系统的驱动下，对这些相对静态的网络安全知识进行清洗、挖掘和推演，构建知识子图库，然后通过高并发知识访存接口，存储到多元时变网络安全知识图谱管理模块中。在每次试验开始前，针对试验配置构建试验场景知识图谱。

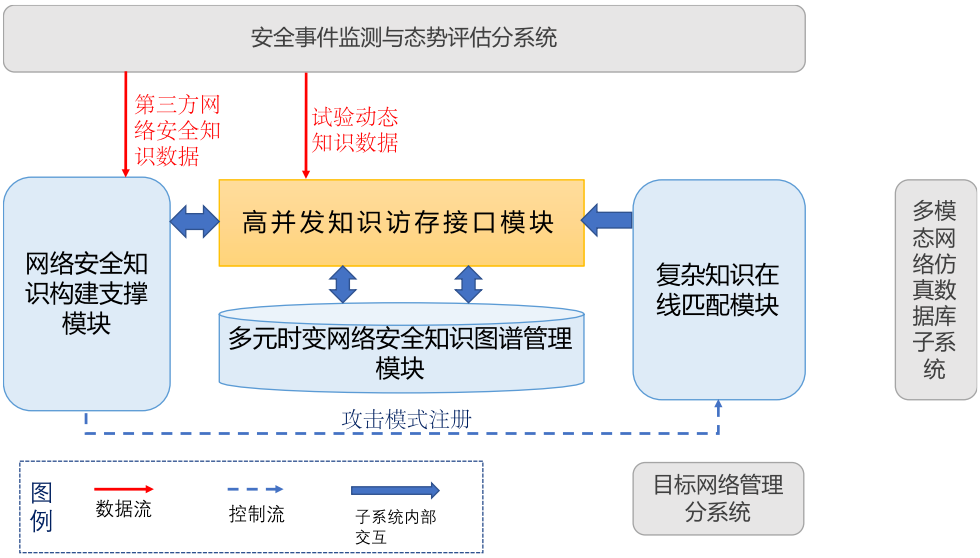


图 6 多元网络安全知识库（试前信息交互）

试验运行阶段，复杂知识在线匹配模块根据试验场景知识图谱，对高速到达的安全事件数据和状态数据进行关联分析，支撑安全事件监测与态势评估分系统发现潜在的复杂攻击事件，将结果通过高并发知识访存接口写入到知识图谱管理模块中。此外，还需为安全事件监测与态势评估分系统提供安全知识数据的实时查询服务，提供网络仿真平台的态势动态知识结果。

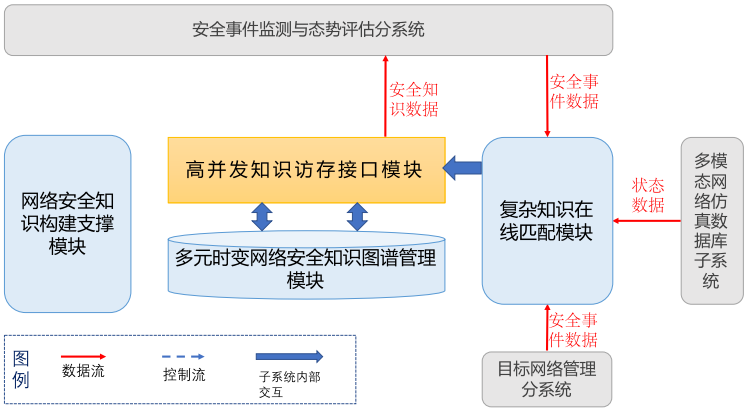


图 7 多元网络安全知识库（试中信息交互）

试验结束后，网络安全知识构建支撑模块为安全事件监测与态势评估分系统提供离线分析的计

算平台，提供攻击模式挖掘程序快速开发框架和分布式运行环境。

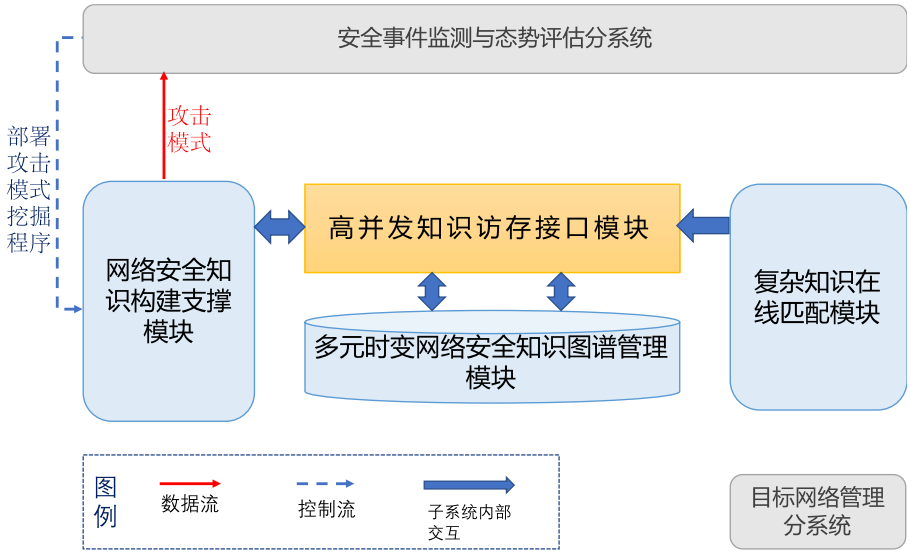


图 8 多元网络安全知识库（试后信息交互）

5.4 子系统功能性能

主要功能要求包括：

1. 提供网络安全知识时空演变、多元复杂关联的表示模型。能够有效表达、存储和索引实体间的多元复杂关联关系，提供同时连接多个实体的超边模型，以及关系属性随时空动态演变的存储与检索模型。此外，每条知识可附带存储一批证据文本，提供“关键词查证据”、“证据查知识”、“知识查证据”等多种高性能检索方式，从而支撑离线知识验证。

2. 具备知识构建的支撑能力，提供基于文本的网络安全知识抽取和基于操作日志的知识抽取基础组件和知识映射框架，为知识子图库的快速构建提供通用知识抽取的基础支撑。

3. 具备多知识图谱的动态构建与管理能力，能够为每次试验构建独立的、具有时空特征的知识图谱，能够对知识子图库和试验场景知识图谱进行联合查询，并提供混合排序、路径搜索等功能。

4. 基于试验场景知识的高并发高速数据流复杂知识在线匹配能力。系统能同时支持多个试验的数据流在线分析，对数据流进行实时统计和已有知识模式的匹配。系统通过 http 协议，实时接收来自业务系统的增量数据，当数据流被处理后，系统根据预先载入的计算脚本得到一个时间窗口可伸缩的计算结果，并将结果保存在分布式存储中。数据计算必须以增量计算的模式实时运行，以保证时效性。

5. 提供知识推演计算的分布式环境，具有便捷的知识推演开发框架和一系列知识推演计算基础组件。支持使用多种分布式计算框架进行全局图分析和批量图处理，提供针对知识计算的磁盘优化布局，从而提升知识离线挖掘与推演的计算速度和稳定性。知识推演计算基础组件方面，包括图聚

类、可达路径搜索等批量迭代式处理算法。

6. 提供 Gremlin 查询接口和知识管理 JAVA 开发接口，能够统一透明地修改、删除和检索知识子图库和试验场景知识图谱。

子系统性能要求如下：

1. 规模方面，支持亿级节点、百万子图规模的知识库存储与管理；支持 1000 个用户并发写入；

2. 查询速度方面，支持 1000 个用户并发查询；支持平均 10 次/s 的并发查询场景，面向业务分系统需求的知识查询平均响应时间小于 100ms；

3. 吞吐量方面，支持 12 小时内的数据流关联分析，检测计算吞吐量大于 20000tps。

5.5 多元时变网络安全知识管理模块

多元时变网络安全知识图谱管理模块支持知识子图库和试验场景知识图谱的统一表达和查询管理需求。

功能要求包括：

1. ★提供同时连接多个（3 个及以上）实体的超边模型，能够有效表达、存储和索引实体间的多元复杂关联关系；（投标方需提供其已有知识库管理系统相关产品的官网介绍截图证明，并加盖公章。截图中，明确可见其产品具有上述功能。）

2. 支持动态时变属性与关系的多值知识数据存储与索引，能够根据特定时空条件快速检索相关实体，能够从特定实体出发快速检索其属性与关系的时空特征，支持按时空属性对节点和边进行快速排序；

3. ★可为每条知识关联一组证据文本数据，支持证据文本数据的快速检索，支持证据数据与知识数据间的关联检索；（投标方需提供其已有知识库管理系统相关产品的官网介绍截图证明，并加盖公章。截图中，明确可见其产品具有上述功能。）

4. 支持 1000 个场景知识图谱、百万个子图的高并发图查询、管理与遍历操作；

5. 提供知识本体可视化编辑工具，支持知识模型、索引配置的在线无缝升级；

6. 提供可视化知识数据管理功能，支持对知识数据的在线编辑、删除、增加等操作；

7. 支持知识数据的批量导入和在线流式写入，在高速流式写入的同时，具备快速检索能力；

8. 支持知识数据的持久化保存，具有多副本备份机制；

9. 支持知识更新的事务操作；

10. 具有 fail-over 和负载均衡能力，能够根据服务器负载和服务器失效情况自动进行数据迁移；

11. 提供自动化部署脚本；

12. 提供服务状态可视化监控功能，能够感知数据状态、数据分布、服务状态、性能状态等。

性能指标包括：

1. 支持 1000 个用户、百万个子图规模的高性能并发查询，并发度平均 10 次/s、峰值 100 次/s；

2. 面向业务系统应用场景的单跳知识查询平均响应时间小于 50ms，2 跳知识查询平均响应时间小于 100ms；

3. 支持亿级节点、十亿级边、百万个子图规模知识数据的高效存储管理；

4. ▲每条知识最高支持 1 万条证据数据，证据检索响应时间小于 100ms；（投标方需提供其已有知识库管理系统相关产品的官网介绍截图证明，并加盖公章。截图中，明确可见其产品可为每条知识存储一组证据数据，且性能能够满足上述指标。）

5. 具有良好的可扩展性，支持 scale-out 分布式集群扩展规模。

5.6 网络安全知识构建支撑模块

该模块包括知识抽取和知识推演两种知识构建方式，具体功能要求包括：

1. 提供基于文本的关系与属性抽取功能，能够从公开文本信息中抽取知识。

2. 提供基于半结构化数据的知识抽取功能，能够从日志数据中还原知识。

3. 提供知识推演的计算框架与计算环境，支撑安全事件监测与态势评估分系统进行网络安全知识缺失边和缺失属性的补齐推演。

4. 提供相似子图搜索、图聚类、路径搜索等基础推演算子，为安全事件监测与态势评估分系统的挖掘推演提供基础支撑。

5. 提供知识融合映射框架，支持多源异构知识库的知识融合；提供可视化的映射规则编辑工具，内置多种智能转换函数。

6. 具有指定公开知识的数据爬取功能，为网络安全知识构建提供原始数据输入。

7. 具备知识图谱的动态构建支撑能力，支撑具有时空特征的知识图谱构建。

8. 针对网络安全知识计算优化磁盘布局，从而提升网络安全知识离线挖掘与推演的计算速度和稳定性。

9. 提供可视化的服务监控工具，可查阅系统服务和作业的运行状态、数据吞吐量和运行日志，可对各类批处理作业进行停止、删除、启动等可视化管理操作。

性能指标：

1. 知识融合与对齐计算的吞吐量不小于每秒 1000 条知识；

2. 指定数据源的采集更新周期小于 24 小时；

3. 支持亿级规模的知识推演计算。

5.7 复杂知识在线匹配模块

复杂知识在线匹配模块的功能要求包括：

1. 支持将试验场景知识图谱转换成在线知识匹配与统计分析脚本。

2. ▲支持基于已有知识对数据流进行高速匹配计算与关联分析；数据计算必须以增量计算的模式实时运行，能够实时处理复杂的逻辑运算，包括时间窗口移动、波动性判断、集中度判断、连续递增、连续递减、复杂事件流等。在进行复杂逻辑处理时，不会对系统的吞吐量造成较大影响。（投标方需提供其已有流数据处理相关产品的官网介绍截图证明，并加盖公章。截图中，明确可见其产品具有上述功能。）

3. ▲支持基于事件驱动的模式识别技术，支持上下文的处理功能，能处理诸如“统计某实体对过去 24 小时最大的事件时间间隔”等问题。（投标方需提供其已有流数据处理相关产品的官网介绍截图证明，并加盖公章。截图中，明确可见其产品具有上述功能）

4. 可灵活配置数据分析时间窗口，最长时间窗口可达到 12 小时。

5. 计算脚本的管理模式是基于脚本包的，且脚本包下还可以创建子包；每个脚本包中可以建立任意多个计算脚本，脚本包可以配置复制、删除，以及读、写、构建的权限管理。

6. 采用基于 Http 协议的数据包接口形式接受数据流，并通过高并发知识访存接口提供结果查询服务。

7. 以可视化界面的形式提供新增、修改指标时的即刻生效功能。

8. 以可视化界面的形式提供系统级、应用级、性能监控，包括平均/最大/最小延迟、TPS、队列堆积、集群健康等指标。

9. 提供编程接口，可通过程序调用对规则进行注册和管理。

10. 支持多服务器节点的集群部署模式。

11. 支持计数、求和、平均、最大、最小、方差、标准差、3 阶中心矩、4 阶中心矩、连续、递增/递减、最大连续递增/递减、采集、过滤等多种分布式实时计算模型。

性能指标包括：

1. 在线匹配与分析支持不小于 1 万个匹配模式；

2. 支持 1000 个用户的并发数据流分析；

3. ★在基于事件序列规则的 2 层跳板机攻击环路检测场景中，单服务器节点、规则数 100 的测试场景下：60 分钟检测窗口数据处理吞吐量大于 1.2 万条/秒，平均延迟小于 5 毫秒；12 小时检测窗口吞吐量大于 1 万条/秒，平均延迟小于 8 毫秒；（投标方需提供其已有流数据处理相关产品的

官网介绍截图证明，并加盖公章。截图中，明确可见其产品能达到上述性能指标。）

4. ▲在基于事件序列规则的 2 层跳板机攻击环路检测场景中，服务器节点 3 个、规则数 100 条，检测窗口 12 小时，数据处理吞吐量达到 2 万条/秒，延迟小于 8 毫秒。（投标方需提供其已有流数据处理相关产品的官网介绍截图证明，并加盖公章。截图中，明确可见其产品能达到上述性能指标。）

5.8 高并发知识访存接口模块

高并发知识访存接口模块功能要求包括：

1. 提供 JAVA 版 Gremlin 查询语言接口，并面向网络仿真验证平台的业务需求，新增证据检索与管理、超边知识检索与管理、时空区间检索、时序排序、关联文档检索与管理、知识编辑、邻接点属性分析、节点属性统计、知识可信度排序等定制接口；

2. 支持嵌入式 JAVA SDK 调用方式和基于 JAVA RMI 独立部署服务方式两种集成方法；

3. 提供面向网络安全知识推演的知识批量加载与批量更新 API 编程接口；

4. 能够对知识子图库和动态知识图谱进行在线融合，提供混合排序、路径搜索、图谱游走、查询结果分页等功能；

5. 支持根据节点查属性、根据属性条件查节点等查询场景；

6. 支持多属性模糊搜索，支持多属性的布尔逻辑组合检索；

7. 提供可视化的知识查询、编辑和管理工具，可进行交互式查询和知识维护操作。

性能指标包括：

1. 支持 1000 个用户同时连接知识库子系统；

2. 支持 1000 个知识访存并发调用，能对调用操作进行排队处理，根据知识图谱管理模块的负载实施知识访存。

6. 多模态网络仿真数据库子系统

6.1 子系统概述

多模态网络仿真数据库子系统为网络仿真平台提供流式结构化数据、流式半结构化数据、流式非结构化数据以及批量非结构化数据等多种模态数据的存储服务和分布式计算环境。

6.2 子系统组成

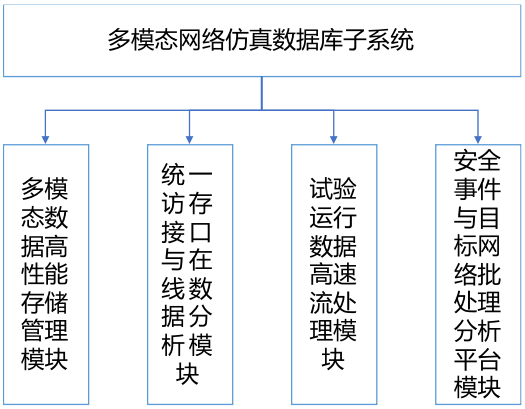


图 9 多模态网络仿真数据库子系统组成图

多模态网络仿真数据库子系统由多模态数据高性能存储管理模块、统一访存接口与在线数据分析模块、试验运行数据高速流处理模块、安全事件与目标网络批处理分析平台模块组成。

多模态数据高性能存储管理模块负责存储管理网络仿真平台中的交互型关系数据、持续文本日志数据、二进制文件数据、持续流式浮点数据、持续流式结构化数据、非持续流式非结构化数据和非持续流量报文数据，并针对数据特点，提供相应的关系型、全文索引型、时序型和多维分析型检索服务。

统一访存接口与在线数据分析模块面向网络仿真平台其他业务分系统的数据访问特点，实现各种物理存储类型的 SQL、POXIS 或 HTTP 访存接口，从而使多模态数据库兼容各种业务模块已有的数据交互模式；此外，还提供多种交互式在线分析工具。

试验运行数据高速流处理平台模块负责对高速到达的状态数据和试验数据进行清洗映射、主键分配、冲突检测与批次聚合，最终实现高性能的一致性写入。

安全事件与目标网络批处理分析平台模块为安全事件监测与态势评估分析系统的分析程序开发和部署运行提供基础组件和管理服务，能够根据配置批量加载系统中的各类数据，并转换为面向业务的数据实体对象，从而使业务相关的分析程序只需关注自身业务逻辑，可基于数据实体对象快速开发分布式分析程序。

6.3 子系统控制与数据流图

该子系统的数据交互与控制逻辑如所以下三图所示。

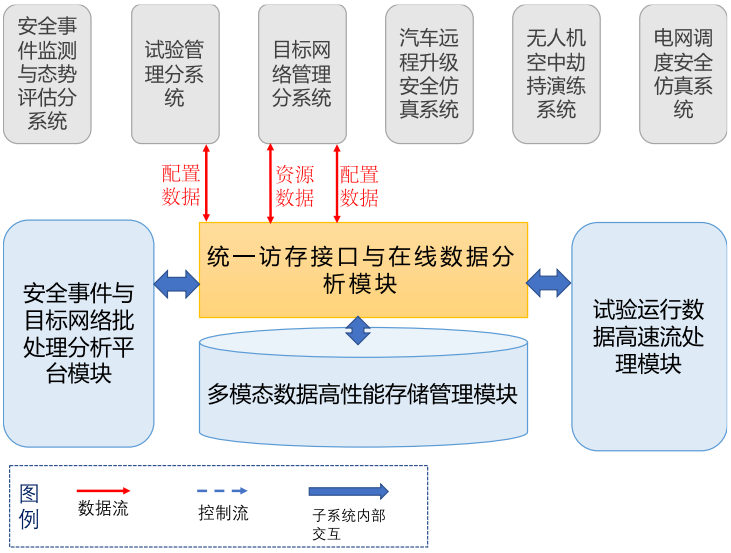


图 10 多模态网络仿真数据库子系统（试前信息交互）

在试前准备阶段，试验管理分系统通过统一访存接口，以 SQL 交互方式，在本子系统中存储和加载试验相关的配置信息、人员信息等试验准备数据。目标网络管理分系统通过统一访存接口，从多模态数据高性能存储管理模块中加载相关的系统资源文件和配置数据，构建目标网络。

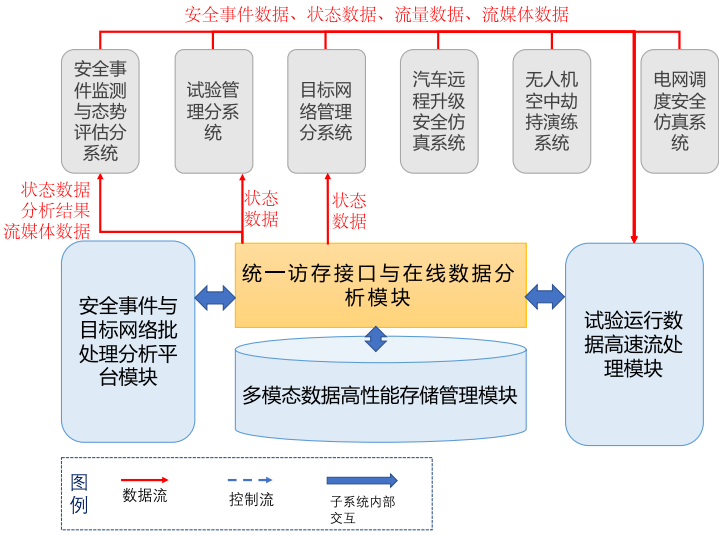


图 11 多模态网络仿真数据库子系统（试中信息交互）

在试验进行阶段，安全事件监测与态势评估分系统、目标网络管理分系统、试验管理分系统、无人机空中劫持演练分系统、汽车远程升级安全仿真分系统、变电站安全仿真分系统将网络流量以及各类探针采集到的状态数据，推送到试验运行数据高速流处理模块，由该模块对数据进行清洗、映射、融合后，形成一致性的数据结构，通过访存接口聚合写入到多模态数据高性能存储管理模块的相应物理存储中。另一方面，安全事件监测与态势评估分系统、目标网络管理分系统、试验管理分系统根据试验监测和导调需要，通过统一访存接口，读取相关实时数据和聚合分析结果。

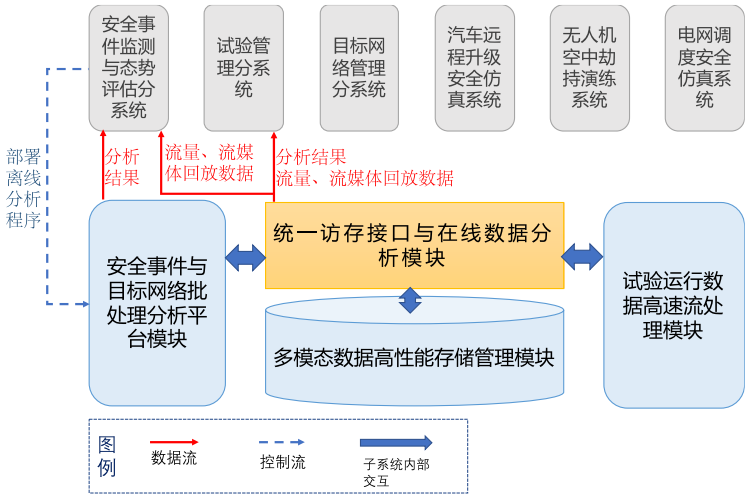


图 12 多模态网络仿真数据库子系统（试后信息交互）

在试验结束后，安全事件监测与态势评估分系统可在安全事件与目标网络批处理分析平台模块中部署离线分析程序，对试验结果进行复杂指标计算和评估分析。试验管理分系统可通过统一访存接口与在线分析模块，读取试验回放数据或查询指定的数据条目，也可调用存储管理模块内置的聚合、分类和多维分析工具，实现简单的在线数据分析。

6.4 子系统功能性能

主要功能要求包括：

1. 为网络仿真平台的结构化、非结构化、流式和离线形态等多种模态的网络仿真数据提供统一高效的数据存储、索引、查询、删除、更新服务；
2. 为批量试验数据离线分析提供分布式计算平台，实现多模态数据的统一批量加载与结果自动更新；
3. 支持网络仿真平台状态数据的高效流式清洗与融合；
4. 提供统一的查询管理接口和多种在线分析工具。

主要性能指标包括：

1. 支持 1000 个用户同时查询或者配置试验参数；
2. 支持 1000 个试验的数据并发写入；
3. 数据并发加载峰值速率达 5000 条/s；
4. 面向业务系统应用场景的数据查询响应时间平均不超过 100ms；
5. 支持试验流量数据的完整保存与回放，存储的平均加载速率不小于 100MB/s。

6.5 多模态数据高性能存储管理模块

多模态数据高性能存储管理模块的功能要求包括：

1. ▲提供原始网络报文数据存储管理服务，能够针对采集的原始网络报文，实现精准的无损

数据包记录，对每个数据包提供纳秒级时间戳，支持 NTP、PTP 获取时间，可以根据应用需求，自定义配置流量回放过程的分流、回放策略，支持多份流量同时复制；（投标方需提供其已有网络报文相关产品的官网介绍截图证明，并加盖公章。截图中，明确可见其产品具有上述功能。）

2. 提供 sFlow 流量数据存储管理服务，支持对大规模 sFlow 数据的快速写入、关联查询和多维统计分析；

3. 提供物理设备状态、虚拟节点状态和设备状态等时序数据的存储管理服务，支持千亿级数据规模；

4. 提供试验配置、试验运行、系统配置和资源元数据的高可靠存储和动态字段索引，支持嵌套 JSON 对象的自动索引；

5. 提供持续文本日志的原始数据存储和索引服务，具有分布式的存储管理、快速检索和聚合分析功能，能支持 PB 级数据规模；

6. 提供镜像文件、软件工具、录屏文件、无人机视频等大文件数据存储管理服务，支持大文件数据的高并发快速访存；

7. 提供面向网络仿真业务的百亿级规模关系型数据存储管理服务，能实现一键水平伸缩，具有强一致性的多副本数据安全、分布式事务、迁移便捷、实时 OLAP 等重要特性；

8. 具有良好的鲁棒性、实时性、可扩展性和可维护性；

9. 具有 fail-over 和负载均衡能力，能够根据服务器负载和服务器失效情况自动进行数据迁移；

10. 提供可视化管理功能，支持对库表结构、索引配置等存储方案的动态创建、修改和更新；

11. 提供自动化部署脚本；

12. 提供服务状态可视化监控功能，能够感知数据分布、性能状态。

性能指标包括：

1. 总数据规模可达 PB 级，关系型数据支持百亿条记录的高可靠存储与快速检索；

2. 能支持 1000 个试验的动态数据并发写入；

3. 静态镜像资源下载吞吐量达 1GB/s；

4. 试验配置数据要支持 1000 用户同时查询或者配置试验参数；

5. 结构化和半结构化数据并发加载峰值速率达 5000 条/s，简单匹配与模糊搜索数据查询单页（小于 100 条）平均响应时间不超过 100ms，面向业务场景的复杂聚合查询平均响应时间小于 3 秒；

6. 支持 10 日内试验运行数据的秒级查询；

7. ★网络报文需支持每年 480TB 数据存储，平均加载速率达到 100MB/s；回放速率峰值可达

1GB/s。（投标方需提供其已有网络报文相关产品的官网介绍截图证明，并加盖公章。截图中，明确可见其产品能够达到上述性能指标。）

6.6 试验运行数据高速流处理模块

试验运行数据高速流处理模块的功能要求包括：

1. 支持基于规则的数据字段映射，提供可视化的数据入库映射规则管理工具；
2. 内置多种数据格式的转换函数，并支持动态扩展函数包进行数据清洗与转换；
3. 支持数据流的多主键冲突检测，能够进行合理的批次规划，在实现高性能批次聚合写入的同时，避免主键冲突导致的写入失败；
4. 提供兼容 kafka 的结构化数据写入接口和基于 Restful 的非结构化文件流写入接口；
5. 对异地分布式仿真平台的数据提供高可靠远程写入接口；
6. 提供可视化监控工具，可感知集群中部署的流处理任务运行状态、数据吞吐量、资源占用情况，并可进行资源分配、启动、停止、部署等管理操作。

性能指标包括：

1. 总吞吐量最高可达 1 万条数据每秒；
2. 支持的映射规则不少于 100 条；
3. 支持的并发试验数不少于 1000 个。

6.7 安全事件与目标网络批处理分析平台模块

安全事件与目标网络批处理分析平台模块的功能要求包括：

1. 提供面向网络安全态势评估分析需求的 Java 版快速开发框架；该框架内置网络仿真试验数据对象操作模型，以及多模态数据统一批量加载、作业管理、计算结果自动更新等基础服务；
2. 提供层次聚类、事件分类、关联挖掘、趋势预测等基础算子；
3. 提供分布式批处理计算环境，内置大规模数据的合并、交集、差集、多表关联等集合运算服务；
4. 提供可视化的批处理分析作业状态监测和管理工具，可进行分析作业程序的部署、运维和管理。

性能指标包括：

1. 支持 PB 级网络仿真平台数据的分布式计算；
2. 批量加载与更新吞吐量大于 100MB/s。

6.8 统一访存接口与在线数据分析模块

统一访存接口与在线数据分析模块的功能要求包括：

1. 所有访存和管理操作，提供统一的 Java RMI 开发接口和基于 Restful 的管理接口，使接口服务实例具有水平扩展能力；

2. 结构化数据支持 SQL 查询语言，半结构化数据支持类 ElasticSearch 的查询语言；

3. 提供内置 Java Bean 实体类，对仿真平台涉及的各类日志、状态、事件、资源、配置等数据对象进行封装；

4. ★针对网络报文数据，提供流式查询、同步回放、进度控制和统计功能；其中，同步回放指多个数据流在一定时间误差内按照原始数据产生的时间序进行回放；进度控制指回放时间点跳转与快进；（投标方需提供其已有网络报文相关产品的官网介绍截图证明，并加盖公章。截图中，明确可见其产品具有上述功能。）

5. 针对试验配置文件，支持多层嵌套的动态索引，可对任意层级的字段进行组合模糊查询，支持数据分页、版本变更历史查询和快照管理；

6. 针对结构化数据提供基于 JDBC 的扩展接口，具备主键查询、关联查询、多属性模糊查询、全文检索、数据分页、聚合查询和时空区间检索等查询功能，以及更新、删除、建表等管理功能；

7. 针对文件类数据，提供文件元数据管理和文件系统服务，支持 HTTP 访问接口，并提供文件系统扩展属性管理接口和文件多版本管理接口；

8. 提供分类、聚类、关联分析、在线联机分析等不少于 5 种可视化交互式分析工具；

9. 提供数据增、删、改、查的可视化界面。

性能指标包括：

1. 支持 1000 个用户和 1000 个试验同时连接多模态网络仿真数据库子系统；

2. 多数据流同步回放时间误差小于 3 秒。

7. 存取性能需求测算

根据各业务分系统的需求，各类数据的存储规模、吞吐量、存储时间详细需求如下各表所示。

1. 配置、运行数据的存取性能要求如表 1 所示：

表 1 配置、运行数据的存取性能要求

数据对象	数据分类	存储规模	加载时延	加载速率	加载峰值	存储时间	实例数量	其他
试验配置数据	交互型关系数据	2000 万条，1TB	小于 100ms	1000 条/s	5000 条/s	永久	1	支持事务处理
试验运		1000 万条，	小于	1000	5000	1 年	1	

行数据		0.5TB	100ms	条/s	条/s			Jpa 规范
系统配置数据		5 万条，<0.1TB	小于 100ms	1000 条/s	1000 条/s	永久	1	
资源元数据		10 万条，<0.1TB	小于 100ms	1000 条/s	1000 条/s	永久	1	

2. 日志类数据存取性能要求如表 2 所示：

表 2 日志类数据存取性能要求

数据对象	数据分类	存储规模	加载时延	加载速率	加载峰值	存储时间	实例数量
系统日志	持续文本日志数据	150TB	秒级	500 条/s	500 条/s	3 月	500
操作日志		15TB	秒级	500 条/s	500 条/s	永久	100
网络仿真平台活动日志		1TB/年	秒级	200 条/s	400 条/s	永久	1
虚拟机内部数据（带外采集）		30TB	秒级	1000 条/s			

3. 业务类数据存取性能要求如表 3 所示：

表 3 业务类数据存取性能要求

数据对象	数据分类	存储规模	加载时延	加载速率	加载峰值	存储时间	实例数量
终端检测数据	持续文本日志数据	652GB	秒级	40 条/s	100 条/s	永久	1000
流量检测数据		3T	秒级	400 条/s	4000 条/s	永久	1
漏洞探测数据		12G	秒级	200 条/s	400 条/s	永久	4
关联分析数据		100G	秒级	50 条/S	100 条/s	永久	400

4. 状态类数据存取性能要求如表 4 所示：

表 4 状态类数据存取性能要求

数据对象	数据分类	存储规模	加载时延	加载速率	加载峰值	存储时间	实例数量
物理设备	持续流式	12 亿浮点数，	秒级	500 条	500 条	1 年	500

状态	浮点型数据	200G		/s	/s		
虚拟节点状态		48 亿浮点数，800G	秒级	2000 条/s	5 万条/s	1 年	400
设备状态数据		1TB/年	秒级	待定	1000 条/s	待定	1000

5. 文件类数据存取要求如表 5 所示：

表 5 文件类数据存取要求

数据对象	数据分类	存储规模	吞吐量	存储时间	实例数量
镜像文件	二进制文件数据	100T	10Gbps	永久	1
软件工具		100T	10Gbps	永久	1
录屏文件、无人机视频文件		300T	10Gbps	永久	1
其他文件		10T	/	永久	1

6. 原始报文数据存取要求如表 6 所示：

表 6 原始报文数据存取要求

数据对象	数据分类	存储规模	加载速率	加载峰值	存储时间
网络报文数据	持续流非结构化数据	216TB	100MB/s	1GB/s	一年

7. 流量日志数据存取要求如表 7 所示：

表 7 流量日志数据存取要求

数据对象	数据分类	存储规模	加载时延	加载速率	加载峰值	存储时间	实例数量
sFlow 流量数据	持续流结构化数据	31.5TB	秒级	100 条/s	2500 条/s	一年	400