DOI:10.13878/j.cnki.jnuist.2017.05.013

乔琪[1]　郑佳佳[1]　许艳萍[2]　何道敬[1]

环境感知应用系统的数据传输与安全

摘要

环境感知应用系统广泛应用在工业生产、日常生活等领域.本文主要研究环境感知应用系统中的数据收集、安全传输和安全管理等技术,提出了环境感知应用系统架构图,包括环境数据采集单元、数据传输网络及云数据中心,从数据的收集、传输、存储、应用、管理等多个方面保护环境数据的安全性.首先,本文阐述了数据在环境感知应用系统中的收集和传输流程,然后,分析数据从环境数据源传输到现场控制单元,再接入互联网传输到云数据中心采用的安全传输方式.最后,研究了可应用于云数据中心的多种安全防护方法以保护数据安全,包括敏感数据加密、数据隔离、访问控制、权限管理、审计日志、备份恢复等.

关键词

环境感知;安全传输;云数据安全防护

中图分类号 TN918.1;TP393.08

文献标志码 A

收稿日期 2017-07-27

资助项目 国家重点研发计划(2017YFB0802805,2017YFB0801701,2017YFB0802302);国家自然科学基金(U1636216,51477056,61601129);国家电网公司科技项目(SGSDDK000KJJS1600065)

作者简介

乔琪,女,博士生,主要研究方向为嵌入式系统信息安全.qqy708@163.com

何道敬(通信作者),男,博士,教授,主要研究方向为网络安全和传感器安全.djhe@sei.ecnu.edu.cn

1　华东师范大学　计算机科学与软件工程学院,上海,200062

2　杭州电子科技大学　计算机学院,杭州,310018

0　引言

随着各种电子设备的飞速发展与迭代,现代生活越来越趋向信息化与智能化.为了更方便地管理和监控设备的运行,人们提出了建立“环境感知系统(Context-aware System)”.环境感知系统能够采集被观测对象的各种信息而不需要获取其目的性信息,因此它对于被观测对象来说是安全的,兼具可用性与有效性.环境感知应用系统的雏形是 Want 等[1]在 1992 年提出的行为徽章定位系统(The Active Badge Location System),处于环境中的相关人员佩戴向中央位置服务传送位置信号的徽章,即中央服务器通过无线传感网搜集环境中人员的位置信息.随后,各种基于不同监测对象的环境感知系统迅速发展了起来.虽然迄今为止位置信息都是最常用的环境感知属性(比如汽车定位系统),但近几年来,需要监控的环境信息也越来越繁杂,比如动力环境感知系统,需要感知设备运行环境的温度、湿度以及红外线照射情况等.

1994 年,Schilit 等[2]首先提出了“环境感知(context-aware)”的概念,他们把附近人员的位置信息、身份标识以及这些信息的更改看作需要感知的环境对象.在环境感知系统研究初期,通常都是这样采用枚举的方式来列举环境属性.1997 年,Ryan 等[3]则把“环境”描述为掌上计算机可感知或者可操控的相关环境信息,比如位置、时间、温度和用户身份.1998 年,Dey[4]把“环境”定义为用户的情绪状态、关注焦点、所处位置及方向、时间日期与用户所处环境内的人或对象.但这些定义还是过于宽泛,不能确切描述环境感知系统的功能.2000 年,Dey[5]给出了一个相对精准的定义,他把环境定义为“在用户和应用交互时,所有可以用来描述包括用户和应用在内的实体(比如人、地点或对象)当前状态的信息”.这些信息包括很多种,比如传感器感知信息、网络信息、设备状态、用户文件访问信息以及其他资源使用信息.

现阶段的环境感知系统主要应用于工业控制、医疗、智能家居和航天器械等领域.

在工业背景下,使用环境感知系统监控工业生产过程,可保证工业系统的安全性.2012 年,Islam 等[6]提供了一个关于工业自动化和控制系统中无线传感网的可靠性和面临的安全威胁的调查.Sadeghi 等[7]在 2015 年提出工业物联网的安全架构.近几年,智能工业系统面

向物联网的应用也开始使用环境感知监控平台,并提出了相关安全架构和挑战[8-9].

在智能家居环境下,环境感知系统可用于感知用户的健康数据,如心跳、运动步数等,以及生活环境的相关数据,如房间温湿度等.2003 年,Cook 等[10]介绍了 MavHome 智能家居架构,它允许家庭作为智能代理.2013 年,Viani 等[11]分析了目前智能家居功能,以分布式智能测量和老年援助 2 大例子,讨论了目前智能家居应用的无线架构.

在医疗设施环境下,随着可穿戴式生物传感器和无线通信技术的飞速发展,环境感知系统可以远程、连续并且实时监测患者的健康状态,然后及时反馈给医护人员,提高医疗效率.2014 年,He 等[12]提出了基于轻量级无线医疗传感安全系统.2016 年,Mohan 等[13]研究提出了本体论的发展,有效地处理以 IT 为基础的医疗系统问题.

在对环境感知应用系统的数据进行安全传输和管理时,主要面临以下 3 方面的安全问题:1)攻击者的多元化:环境感知应用系统作为重要的监测系统,吸引着来自社会各界的攻击者,比如敌对军事势力、恐怖组织、政府部门甚至是恶意报复社会的个人.2)入侵方式的多样化:环境感知应用系统有固定的拓扑形式、数据传输模式和相对简单的交互需求,但系统节点种类繁多,环境感知系统可能受到来自各类通信网络、现场总线、移动介质、越界接入等途径的攻击.3)攻击方式的专业化:针对环境感知系统的攻击在过去的 10 多年中已经发生过很多次,比如 Stuxnet、Night Dragon、Duqu 和 Nitro 3 等病毒都专门针对系统的某一特征或功能进行攻击,这充分说明了针对环境感知系统的攻击已经渐趋专业化、明确化,比传统的信息攻击大大地提高了攻击效率.因此,本文针对环境感知系统中的数据安全进行研究,针对数据的安全传输和管理提出了相应的防护措施.

本文主要研究环境感知应用系统中的数据收集、安全传输和安全管理等技术,提出了环境感知应用系统架构图,包括环境数据采集单元、数据传输网络及云数据中心.环境数据采集的方式包括内置传感器采集和基于中间件采集;环境数据从环境数据源传输到现场控制单元包括总线和无线传感 2 种方式,然后通过有线或无线接入网接入到互联网,传输到云数据中心;云数据中心采用多种安全防护方法保护数据安全,包括敏感数据加密、敏感数据隔离、访问控制、权限管理、审计日志、备份恢复等.

本文内容安排如下:第 1 章介绍了环境感知系统的原理及架构,描述了系统中各部分设施的工作情况;第 2 章介绍了数据采集和传输,讨论了环境数据采集和数据传输方法;第 3 章介绍云数据中心数据安全防护方法;第 4 章,展望了环境感知应用系统未来的发展方向.

1 环境感知应用系统架构

环境感知应用系统有很多种部署方式.考虑到不同应用场景下环境感知应用系统的工作环境各不相同,在实际使用中,部署方式的选择主要取决于现场的特殊要求或条件,如传感器网的拓扑方式(本地或远程)、潜在的用户数量(一个或多个)、所使用设备的可用资源(高性能 PC 机或小型移动设备)以及所监控系统的扩展设施等.环境感知应用系统是 C/S 架构,如图 1 所示(环境数据采集单元有 2 种架构,图 1 中仅表达基于中间件方式的环境数据采集单元).其中,客户端是指部署在自然环境中的环境数据采集单元,用来收集自然环境中的数据;服务器是指部署在云端的云数据中心,用来存储环境数据采集单元采集的数据;环境数据通过安全网络链路从客户端传输到服务器端.

环境数据采集单元包括环境数据源和现场控制单元.环境数据源包括但不限于传感器,用来采集设备环境中的环境数据,如水浸程度、烟雾浓度、温度、湿度等.一个现场控制单元能够控制管理多个环境数据源,对环境数据源采集的数据进行汇整,并且按照预定义的格式对汇总的数据进行统一格式转换及初步的数据分析.环境数据源将数据传输到现场控制单元的方式包括有线和无线 2 种方式,有线方式指数据通过总线传输,无线方式指数据通过无线传感网络传输.之后,现场控制单元通过有线或无线的方式接入到互联网中,将环境数据传输到云数据中心.

云数据中心主要实现功能是数据存储、数据管理和数据安全防护.数据存储主要有视频数据存储、图片数据存储、结构化数据存储、半结构化数据存储等方式.数据管理主要实现数据索引、数据融合、数据分析、数据展示等功能.数据安全防护主要针对敏感数据加密、敏感数据隔离、访问控制、权限管理、备份恢复、审计日志等.

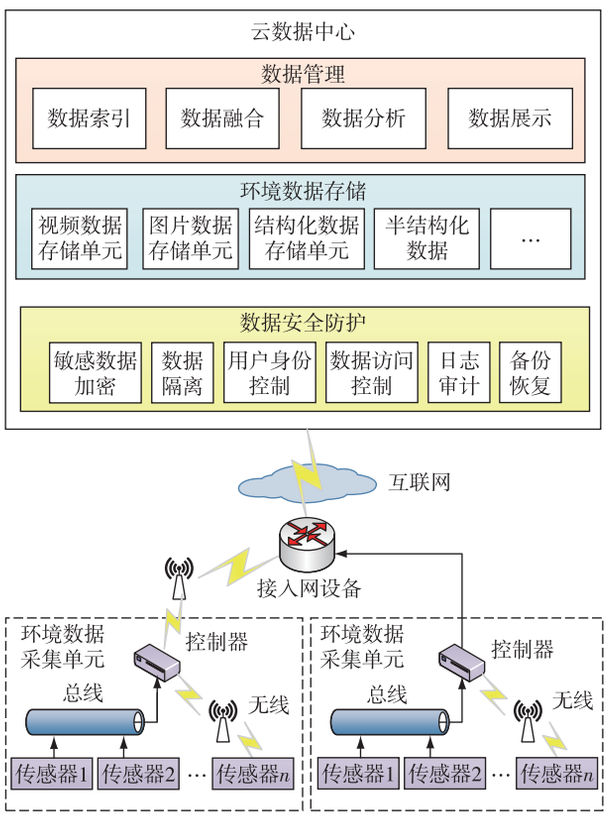

图 1　环境感知应用系统架构

Fig. 1　Architecture of environment-aware application system

2　数据采集和安全传输

2.1　环境数据采集

数据采集主要采用 2 种方式实现:内置传感器采集和基于中间件采集.

1)内置传感器采集方法:内置传感器采集方法通过设备本地内置的传感器收集环境信息,例如:水浸传感器、烟雾传感器、红外传感器、温度传感器等,设备直接收集数据发送给数据中心,没有用于获取和处理传感器数据的附加层.

2)基于中间件的数据采集方法:基于中间件的数据采集方法是对下层传感器采集数据的方法进行封装,隐藏感知细节,从而增加了感知系统的可用性与可重用性.中间件对传感器采集的环境数据进行分析和格式转化处理,然后传送到云数据中心,减少了数据中心处理分析数据的负担,提高了整个系统的工作效率.

2.2　环境数据传输

环境数据的传输过程大致经历以下 2 个阶段:1)环境数据由环境数据源收集完成,从环境数据源传输到现场控制单元包括总线和无线传输 2 种方式;2)现场控制单元将环境数据通过接入网设备接入到互联网,传输到云数据中心.如图 2 所示.

数据由最底层环境数据源产生,通过有线或无线的方式传输至现场控制单元进行数据预处理,有线指数据通过总线传输,遵循总线协议,如 CAN 协议、HART 协议等;无线指通过无线传感网传输数据,主要遵循 Zigbee 协议.预处理一般完成不同传感器产生的数据的统一格式转换.转换的数据通过有线或无线的方式接入网,无线方式主要包括蓝牙、WiFi、Zigbee、移动通信网络和 WiMax 等.数据从现场控制单元到云数据中心的安全传输方式主要采用 VPN 传输、HTTPS 传输等.数据存储、数据分析、数据管理以及数据安全防护在云数据中心实现.

2.2.1　环境数据源与现场控制单元之间的数据传输

1)有线方式

环境感知应用系统的环境数据采集单元使用有线传输方式指的是环境数据源通过总线将感知数据

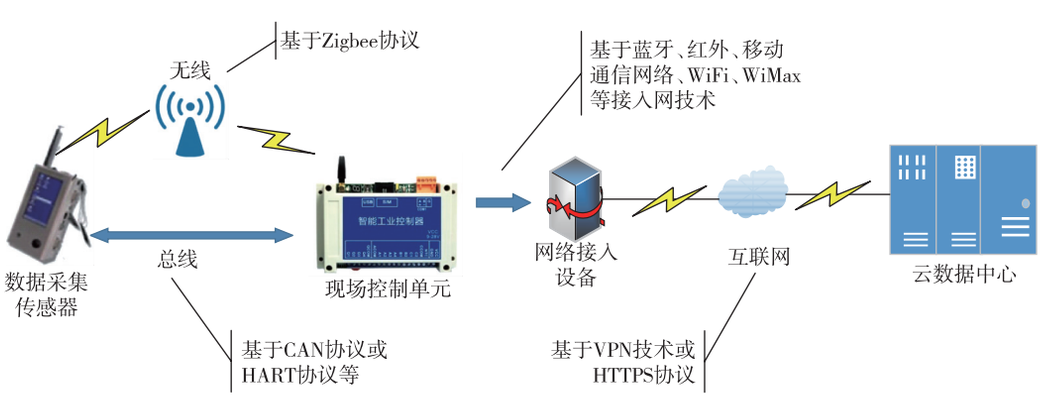

图 2　传感数据安全传输方式和过程

Fig. 2　Safe transmission process of context data collected by sensors

传送至控制器.使用总线需遵循总线协议,环境感知应用系统中总线传输一般基于2种协议,一是CAN总线协议,二是HART协议.

CAN总线协议能有效地支持分布式控制或实时控制的串行通信网络,总线协议具有高保密性.CAN总线利用率和传输速率高,并且具有可靠的错误检测处理机制,具有很高的安全性.

HART协议是可寻址远程传感器高速通道的开放通信协议.HART协议提供具有相对低的带宽,适度响应时间的通信.其特点是在现有模拟信号传输线上实现数字信号通信.

在环境感知应用系统中,使用CAN总线保证数据的传输速率,其可靠性和安全性也高于无线方式传输,但感知的范围有限,需要结合无线方式弥补不足之处.

2)无线方式

在环境感知应用系统的环境数据采集单元若采用无线传输方式,相当于无线传感网收集信息,大多采用Zigbee协议.Zigbee协议栈主要适用于自动控制和远程控制的工业现场,支持地理定位功能,并且可以抵抗工业现场的各种电磁干扰.Zigbee协议的特点是功耗低、可靠性高、抗干扰性强、布网容易、动态组网、自动路由.Zigbee协议是目前影响最深远的、最为成熟的一种协议.无线传感网方式适用于感知范围广的环境感知应用系统.

2.2.2 现场控制单元和云数据中心之间的数据传输

现场控制单元将环境数据通过接入网设备接入到互联网,传输到云数据中心.接入网技术,主要包括蓝牙、红外、无线上网技术、RFID等,有各自的优势和适用场景.WiFi使用802.11协议;蓝牙使用802.15协议,有短距离、低功耗的特点;RFID遵循ISO/IEC制定5种频段的空中接口协议.以上接入网的技术都有安全性的需求,需要进行接入认证.一种简单有效的认证方式是动态口令认证,即每次使用前都加入不确定因子进行单向函数变换,再由认证方通过相同的函数变换进行数据比对,从而实现接入网的安全认证.

2.2.3 核心网络安全传输

1)VPN传输

环境感知应用系统的核心网络传输采用VPN技术保证数据的安全性.VPN技术的核心是隧道技术,即在网络提供商提供的公用网络上建立专用网络,通过隧道协议对数据加密进行通信.隧道协议中,包括工作在OSI模型第2层的隧道协议,如PPTP(点对点隧道协议)、L2TP(第2层隧道协议)等,以及第3层隧道协议,如GRE(通用路由封装)、IPsec等.前几种协议主要侧重封装,IPsec协议则侧重数据的安全性,结合加密、认证和数据防篡改等多种技术形成了完整的体系,保证IP分组的私有性、完整性和真实性.

2)HTTPS传输

HTTPS是安全超文本传输协议,即基于SSL(Secure Socket Later,安全套接层协议)加密的HTTP协议.SSL协议介于应用层与传输层之间,对明文传输的HTTP数据进行加密后再传输,从而确保通信数据不易被截获和破解[14].SSL协议使用公钥加密技术进行初始化连接,然后传送方使用对称加密技术对HTTP数据进行加密并使用数字签名技术签名,经由TCP/IP传输,由数据接收方进行解密并验证签名.通过SSL加密,一方面建立了安全数据通道,保证了数据传输的安全;另一方面则保证了通信双方的身份真实性,解决了伪装攻击等对数据安全造成的威胁.

3)加密传输

在环境感知应用系统中,数据采集端并没有对传输数据进行加密,因此为保证数据不被泄露,并考虑到传感器和现场控制单元的计算、存储和通信能力有限,系统应采用尽量简单而有效的加密算法,比如移位替换加密、矩阵变位加密等.并且为了避免简单加密安全性差的问题,可以将多个简单加密方法组合起来,比如在基于矩阵变位加密的基础上采用分组加密方法,即采用不同的矩阵对应关系进行分组,这就避免了简单加密中明文与密文具有固定对应关系的问题.

3 云数据安全防护

云数据中心给环境感知应用系统提供了低成本的存储和计算资源的同时,也需要应对着来自各方面的挑战.如文献[15]所述,云数据中心主要面临的数据威胁如下:服务的可用性(Availability of Service)、数据锁定(Data Lock-in)、数据保密和可审计性(Data ConfidentiaIity and Auditability)、数据传输限制(Data Transfer Bottlenecks)、性能不可预知性(Performance Unpredictability)、大规模分布式系统漏洞(Bugs in Large-scale Distributed Systems)、声誉共享(Reputation Fate Sharing)以及软件许可(Software Li-

censing)等.这些威胁都与数据保密性和可靠性相关.为了保护存储在云数据中心的感知数据安全,可以采用数据加密与隔离、身份认证、数据访问控制、日志审计和备份恢复等数据安全防护措施.

3.1 敏感数据加密

云数据中心存储了大量环境感知数据,其中有些数据是敏感数据,比如用户个人信息、保密场所的图片数据等,因此需要对环境信息中的敏感数据进行加密以保证用户安全.除了上文提到的在数据传输过程中进行加密以外,数据加密还可以在数据存储过程中进行.数据的加密存储通常与检索技术结合在一起,通过数学模型算法完成.比如线性检索算法,首先对原始的环境数据信息进行加密,然后再针对数据的关键字段对密文进行随机排序,进一步生成校验序列,完成数据加密数据的检索.安全索引算法则是在数据加密完成后,基于加密密钥建立索引,将该索引放入布隆过滤器,根据用户读取数据请求进行布隆检测,返回对应的加密数据,对其解密则可获取用户所请求的数据.

3.2 数据隔离

云数据通常采用共享式存储设备,基于虚拟技术对用户数据进行共享存储,较之从物理层对数据进行有效隔离的方式,共享存储方式节约了存储空间,同时保证了用户资源的高效存取效率,但共享存储方式需要确保数据之间相互隔离.目前比较成熟的3种用于云端数据隔离的数据库架构为共享表架构(Shared Schema Multi-Tenancy)、分离数据库架构(Separated Database)和分离表架构(Shared Database Separated Schema)[16],三者主要的区别是是否共享数据库实例和数据库表.共享表架构共享相同的数据实例和数据库表,分离数据库拥有独立数据库实例,分离表架构则共享数据实例但拥有独立数据库表.3种方法对数据隔离和容灾备份都有不同的存储实力和容错性,具体部署时可根据客户数量、隔离性和安全性指标的综合权衡来决定使用合适的数据库架构.

3.3 身份认证

用户身份认证即在用户请求登录云数据中心时验证用户身份,对用户请求做出相应决策,保证云数据中心的访问策略能够有效执行,预防攻击者的伪冒及窃取权限等攻击.最常用的身份认证方法也是口令认证,分为静态口令和一次性口令,系统通过验证请求接入用户输入的用户名与密码是否与系统中预存的用户名与密码完全一致,如果用户身份验证未通过将无法访问申请访问的信息,从而保障云端数据的访问安全.进一步可以使用加密算法如数字签名、消息认证码等以及通信协议来验证用户身份.而针对云数据中心泛在接入(即任意时间任意地点都可能有任意终端设备接入云环境)的特性,最好采用多因子强认证的方法,通过增加用户认证属性(如指纹、声纹等生物特征)来完成用户身份认证.

3.4 数据访问控制

在环境感知应用系统中,环境数据源与现场控制单元等设备和设施组成了一个系统管理员能完全控制的网络,其中所有的数据资源都处于系统管理员的控制之下.但当环境数据上传到云数据中心之后,由于云数据平台多由云服务提供商控制,环境感知应用系统管理员不能完全控制对云数据中心存储的环境数据的存取和使用.对于云数据中心的访问控制可以引入基于角色的思想,根据不同的用户进行角色划分,然后根据角色划定可访问数据范围.具体操作时,对所有用户采用访问控制列表进行统一管理,对超级用户(比如云服务提供商)则结合强制访问控制手段,保证数据访问控制方法灵活性高的同时,解决超级用户行为无法限制的问题.

3.5 日志审计

日志审计即通过采集云数据中心的系统安全事件、用户操作记录、系统运行状态等各种信息,经过整合和标准化处理,对系统日志进行统一化存储和集中管理;通过分析、过滤和归并分析系统日志等处理,快速发现云数据中心所面临的潜在威胁与实时攻击.针对云数据中心日志来源的多样性,系统日志审计模块需要采用可扩展的灵活性采集模式,然后进行规范化存储,并对系统日志进行高效分析与挖掘,获取警告信息以预防数据安全威胁.日志审计技术可以快速定位系统故障,并提供危害来源追查和数据恢复依据.

3.6 备份恢复

云数据中心采用的是分布式存储,较之传统的集中式物理存储方式,它面临的物理安全威胁相对较少,但也不可避免地会出现存储设备故障的问题,因此数据备份和恢复也是必不可少的.数据备份主要有2种方式:物理备份和逻辑备份.其中,物理备份可以采用联机备份即热备份,可以在系统持续工

作的情况下进行备份.逻辑备份则是对数据库对象进行二进制文件抽取的过程,可以作为对物理备份的补充.通过异地物理备份与逻辑备份结合,最大限度地保存系统数据,在故障发生后及时通过镜像技术等手段从分支备份中恢复数据,维持数据中心正常运行.

4 总结

环境感知应用系统渐趋智能化与自动化,应用前景十分广泛,例如军事领域、航天器械和工业控制等方面,受到社会各界的广泛关注.虽然目前关于环境感知应用系统数据采集和传输以及云数据中心的研究成果和实际应用层出不穷,但是仍然没有形成通用的体系和标准.对于环境感知应用系统各个方面的综合研究只是刚刚起步,而随着研究的深入以及投入使用后的反馈,其中隐藏的问题也会逐渐暴露,因此还需要对这个系统从原理、构架、整体管理等方面进行深入的研究.

参考文献

References

[1] Want R,Hopper A,Falcao V,et al.The active badge location system[J].ACM Transactions on Information Systems,1992,10(1):91-102

[2] Schilit B N,Theimer M M.Disseminating active map information to mobile hosts[J].IEEE Network,1994,8(5):22-32

[3] Ryan N,Pascoe J,Morse D.Enhanced reality fieldwork:The context-aware archaeological assistant[J].Computer Applications in Archaeology,1997:269-274

[4] Dey A K.Context-aware computing:The CyberDesk project[C]//Proceedings of the AAAI 1998 Spring Symposium on Intelligent Environments,1998:51-54

[5] Dey A K.Providing architectural support for building context-aware applications [D]. Atlanta, GA: Georgia Institute of Technology,2000

[6] Islam K,Shen W M,Wang X B.Wireless sensor network reliability and security in factory automation:A survey [J].IEEE Transactions on Systems,Man & Cybernetics,Part C,2012,42(6):1243-1256

[7] Sadeghi A R,Wachsmann C,Waidner M.Security and privacy challenges in industrial Internet of Things[C]// 52nd ACM/IEEE Design Automation Conference,2015:54

[8] Sajid A,Abbas H,Saleem K.Cloud-assisted IoT-based SCADA systems security:A review of the state of the art and future challenges [J]. IEEE Access, 2016, 4:1375-1384

[9] Durresi M,Durresi A.Security based cyber-physical architecture for environment protection[C]//IEEE International Conference on Broadband and Wireless Computing,Communication and Applications,2015:43-50

[10] Cook D J,Youngblood M,Iii E O H,et al.MavHome:An agent-based smart home[C]//IEEE International Conference on Pervasive Computing and Communications,2003:521-524

[11] Viani F,Robol F,Polo A,et al.Wireless architectures for heterogeneous sensing in smart home applications:Concepts and real implementation[J].Proceedings of the IEEE,2013,101(11):2381-2396

[12] He D J,Chan S,Tang S H.A novel and lightweight system to secure wireless medical sensor networks[J].IEEE Journal of Biomedical & Health Informatics,2014,18(1):316-326

[13] Mohan P,Singh M.Security policies for intelligent health care environment[J].Procedia Computer Science,2016,92:161-167

[14] 张恒伽.基于中间人攻击的 HTTPS 协议安全性分析[D].上海:上海交通大学信息安全工程学院,2009
ZHANG Hengjia.Security analysis of HTTPS protocol based on MITM attack[D].Shanghai:College of Information Security,Shanghai Jiao Tong University,2009

[15] Armbrust M,Fox A,Griffith R,et al.Above the clouds:A Berkeley view of cloud computing[J].Eecs Department University of California Berkeley,2009,53(4):50-58

[16] 杨旭.基于云计算的数据安全性研究[J].移动通信,2013(9):69-72
YANG Xu.Research on data security based on cloud computing[J].Mobile Communications,2013 (9):69-72

A survey on security of data transmission in context-aware application system

QIAO Qi[1] ZHENG Jiajia[1] XU Yanping[2] HE Daojing[1]
1 School of Computer Science and Software Engineering, East China Normal University, Shanghai 200062
2 School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou 310018

Abstract The context-aware application system is widely used in industrial production and our daily lives. This paper mainly focuses on aspects related to the context-aware application system, such as data collection, secure data transmission & management, and constructs the architecture of the context-aware application system, including the context data acquisition unit, the data transmission network and the cloud data center. The data are collected by sensors, and transmitted to the field supervision unit, then to the cloud data center by the Internet, of which the whole processes are secured through various security protection methods, including sensitive data encryption & isolation, access control, authorization management, audit logs, and backup & recovery. Security of context data is emphasized and practiced in the whole data processes from data collection to data transmission, storage, application, management and so on.

Key words context-aware; security of transmission; cloud data security