DOI ：10.12142/ZTETJ.201903006

网 络 出 版 地 址 ：<http://kns.cnki.net/kcms/detail/>34.1228.TN.20190612.0847.002.html

网 络 出 版 日 期 ：2019-06-12

收 稿 日 期 ：2018-12-28



1, 2

1, 2

[1]

万 物互 联 背景 下 的边 缘 计 算安 全 需求 与 挑战 Security Requirements and Challenges in Edge Computing for Internet of Everything

马 立 川 /MA Lichuan ，裴庆 祺 /PEI Qingqi ，肖慧 子 /XIAO Huizi

1, 2

(1. 西 安 电 子 科 技 大 学 综 合 业 务 网 理 论 及 关 键 技 术 国 家 重 点 实 验 室 ，陕西 西 安 710071 ；

2. 西 安 市 移 动 边 缘 计 算 及 安 全 重 点 实 验 室 ，陕西 西 安 710071 ）

(1. State Key Laboratory of Integrated Services Networks, Xidian University, Xi ’an 710071, China;

2. Xi ’an Key Laboratory of Mobile Edge Computing and Security, Xi ’an 710071, China)

摘 要 ：作为 万 物 互 联 时 代 新 型 的 计 算 模 型 ，边缘 计 算 具 有 的 分 布 式 、“数据第一 入 口 ”、计算

和 存 储 资 源 相 对 有 限 等 特 性 ，使其除 了 面 临 信 息 系 统 普 遍 存 在 网 络 攻 击 之 外 ，还不可 避 免 地

引 入 了 一 些 新 的 安 全 威 胁 。 为 此 ，从4 个 方 面 对 边 缘 计 算 的 安 全 需 求 进 行 阐 述 ，同时对 其 主

要 安 全 技 术 的 设 计 以 及 实 现 所 面 临 的 挑 战 进 行 分 析 ，较为 全 面 地 指 出 了 边 缘 计 算 在 身 份 认

证 、访问控 制 、入侵检 测 、隐私保 护 、密钥管 理 中 存 在 的 具 体 安 全 问 题 。

关 键 词 ：万物 互 联 ；边缘计 算 ；安全需 求 ；隐私保 护

Abstract : As a new computing paradigm in the Internet of Everything, edge computing has

the following characteristics: distributed, data first entry, relatively limited of computing and

storage resources. These characteristics bring some new security threats and network

attacks to the edge computing. In this paper, the security requirements of edge computing

are elaborated from four aspects, and the design of its main security technology and the

challenges are also analyzed. It comprehensively points out the specific security issues of

edge computing in identity authentication, access control, intrusion detection, privacy

protection and key management.

Key words: Internet of Everything; edge computing; security requirements; privacy preserving

1 万 物 互 联 背 景 下 从 云到 边 缘 的 演 变

能力，将人和信息融入到互联网中， 该趋势使得人类社会正在迈入万物 互联（IoE）的时代 。

长 。到 2020 年，连接 到网络的 无 线 设 备 数 量 将 达 到 500 亿 台 ，生 成 的 数据量达到 507.9 ZB。

随

着 单 片 机 嵌 入 式 系 统 和 无 线 通 信 技 术 的 发 展 ，物 联 网技

万物互联的核心在于收集来自 于 终 端 设 备 的 海 量 数 据 ，利用 以 大

目 前 ，海量数 据 的 存储和 处理 主 要 依 赖 于 集 中 式 的 云 计 算 模 型 ，

术 近 年 来 得 到 了 长 足 的 发 展 和 普 及，其实际应用包括智能家居、智慧 交 通 、无 人 驾 驶等 。 近年 来 ，除 了 “ 物 ”与“物”的互 联 ，还增 加 了“物 ” 与“人 ”的互联，其显著特点 是“物” 端具有更强的计算能力和语境感知

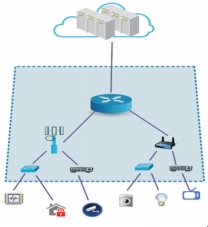
数据、机器学习、深度学习为代表的 智 能 技 术 ，去满 足 不 同 行 业 的 业 务 需求，如制造、交通、医疗、农业等各 行 各 业 。 在 此 背 景 下 ，所需 要 连 接 的终端设备数量达到数十亿甚至数 万 亿 ，其 产 生 的 数 据 呈 爆 炸 式 增

其特征主要表现为数据和存储均位 于 部 署 在 偏 远 地 区 的 云 计 算 中 心 。 尽管云数据中心以堆叠硬件的方式 具 有 较 强 的 计 算 和 存 储 能 力 ，但是 万 物 互 联 背 景 下 ，网络 边 缘 的 终 端 设 备 产 生 的 数 据 已 经 达 到 海 量 级

2019 年 6 月 第 25 卷 第 3 期

中 兴 通 讯 技 术 Jun. 2019 Vol. 25 No. 3

37



[2]

[3]

专 题

万 物 互 联 背 景 下 的 边 缘 计 算 安 全 需 求 与 挑 战

ZTE TECHNOLOGYJOURNAL

马 立 川 等

别，这给云计算模型带来以下挑战： （1）线 性增 长的 集中 式云 计算 能力 无法匹配终端所产生数据的指数增 长 需 求 ；（2）海量数 据 传 输 到 云 计 算中心急剧增加了传输带宽的负载 量，造成较大的网络时延，这给对时 延敏感的应用场景（如无人驾驶、工 业 制 造 等）带 来 了 严 峻 的 挑 战 ；（3） 终 端 设 备 电 能 有 限 ，数据 传 输 会 造 成 电 能 消 耗 较 大 。 为 此 ，集中 式 的 云计算模型已经无法满足万物互联 下的海量数据的高效传输以及处理 需求。

在 此 背景 下，边缘 计算 作 为一 种 新 的 计 算 模 式 ，架起 物 联 网 设 备 和 数 据 中 心 之 间 的 桥 梁 ，使数 据 在 源 头 附 近 就 能 得 到 及 时 有 效 地 处 理。如图 1 所示的基于物-边缘-云 的 三 层 服 务 交 付 架 构 ，将从 数 据 源 到云计算中心数据路径之间的任意 计 算 、存储、网络 资 源 ，形成高 度 虚 拟化平台的“边缘层”为用户提供服 务 ，其中 的 每 层 都 具 有 灵 活 性 和 可 扩 展 性 ，可以 按 需 增 减 相 应 数 量 的 实 体 。 边 缘 计 算 出 现 之 前 ，微云 计

云

边 缘

算 、雾计 算 和 移 动 边 缘 计 算 等 几 种 方法都是利用相似的思想为云计算 提 供 了 补 充 解 决 方 案 。根 据 2018 年 11 月 发布 的《边缘 计 算参考 架构 3.0》所 述 ：边 缘 计 算 模 型 具 有 分 布 式、“数据第一入口”、计算和存储资 源相对有限等特性。

然 而 ，网络边 缘 侧 更贴近 万物 互联的终端设备。由于终端设备的 开 放 性 和 异 构 性 ，以及 相 对 有 限 的 计 算 和 存 储 资 源（与 云 计 算 中 心 相 比），使得访问控制和防护的广度和 难 度 大 幅 提 升 。 此 外 ，边 缘 计 算 还面临信息系统中普遍存在的网络 攻 击 威 胁 。 为 此 ，跨越 云 计 算 和 边 缘 计 算 之 间 的 纵 深 ，实施 端 到 端 的 防护，全方位保障边缘计算的安全， 增 强 其 抵 抗 各 种 安 全 威 胁 的 能 力 ， 是边缘计算促进万物互联进一步发 展的前提和必要条件。

2 边 缘 计 算 安 全 需 求

安全是指达到抵抗某种安全威 胁 或 安 全 攻 击 的 能 力 ，横跨 云 计 算 和 边 缘 计 算 ，需要 实 施 端 到 端 的 防 护。万物互联系统在紧密耦合网络 系统与物理世界中的关键性作用决 定了安全属性和隐私保护的相关需 求要比在以往任何信息系统中更加 重要。

2.1 边 缘 计 算 安 全 的 必 要 性

万物互联系统中终端设备具有 超 大 规 模 、低成本 设 计 、资源受 限 、 设 备 异 构 等 特 性 。 同 时 ，开发 商 重

具挑战性。

目 前 ，边缘计 算 面 临巨大 的安 全 威 胁 。 文 献 [4] 中 ，作 者 分 析 了 2 个利用边缘计算应用场景的安全问 题。一个是在智能制造工厂的场景 下，攻击者可以篡改通信数据包，注 入 伪 造 的 压 力 测 量 值 欺 骗 决 策 器 ， 延迟控制阀门的动作并造成设备损 坏 。 如 果 没 有 适 当 的 安 全 防 范 措 施，不仅生产过程可能中断，工人的 生命在很大程度上受到威胁。另一 个则是移动边缘计算中无人机操作 的 安 全 问 题 ，可以 产 生 模 拟 的 全 球 定 位 系统（GPS）信 号 误 导无人 机 系 统 组 件 ，使其 驾 驶 到 目 标 区 域 以 达 到捕获的目的。作者用无人机实验 验证并达到了在不产生附加损失的 情况下友好地捕获了非合作性无人 机的目的。

在 文 献 [5] 中 ，华盛顿 大 学 计 算 机科学与工程系的科研人员对配备 智能电子控制系统的典型豪华轿车 进 行 了 实 验 安 全 分 析 ，发现 其 安 全 保护系统具有很多设计时就存在的 安 全 漏 洞 ，同时 并 不 是 车 上 的 所 有 组 件 都 遵 循 其 自 己 设 计 的 安 全 协 议 ，这使 得 实 验 人 员 能 够 轻 易 地 侵 入 车 辆 引 擎 控 制 模 块 、电子 刹 车 控 制模块等性命攸关的重要车辆控制 部 件 ，从而 远 程 控 制 行 驶 车 辆 的 油 门、刹车等。

2017 年 6 月 1 日 正 式 生 效 的 《中华人民共和国网络安全法》特别 强调了关键信息基础设施的运行安 全 ，而能源 、交通、制造 等 关 键 基 础

IoT ：物联 网

IoT 设 备 和

传 感 器

视 功 能 优 于 安 全 的 事 实 、用户 更 高 的 隐 私 要 求 、更难 的 信 任 管 理 使 得

设施的工业控制环境无疑将是安全 建 设 的 重 中 之 重 。 2016 年 中 国 信

▲ 图 1 物 -边 缘 -云 三 层 服 务 交 付 架 构

保证万物互联系统的安全性显得更

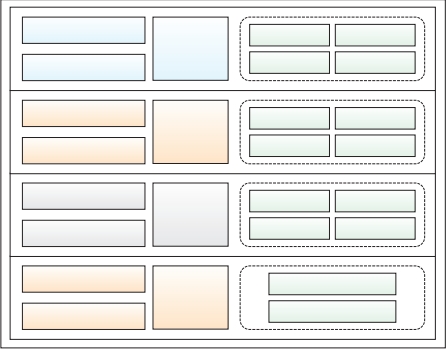
息 通 信 研 究 院 云 计 算 白 皮 书 指 出 ：

38

中 兴 通 讯 技 术

2019 年 6 月 第 25 卷 第 3 期

Jun. 2019 Vol. 25 No. 3



运 行 威 胁

拒 绝 服 务 攻 击

虚 假 边 缘 中 心

协 议 漏 洞

恶 意 节 点

海 量 联 结 与 自 动 化 运 维

实 时 联 接

网 络

安 全

隐 私 泄 露

统 一 身 份 管 理

访 问 控 制

系 统 管 理

入 侵 检 测

边 缘 行 业 应 用

边 缘 业 务 运 营

应 用

安 全

数 据 安 全 存 储

安 全 计 算

可 信 计 算

数 据 分 析 与 呈 现

数 据 聚 合 与 互 操 作

数 据

安 全

操 作 系 统

基 础 设 施

物 理

安 全

自 然 灾 害

马 立 川 等

万 物 互 联 背 景 下 的 边 缘 计 算 安 全 需 求 与 挑 战

ZTE TECHNOLOGYJOURNAL

专 题

公有云服务提供商向用户提供大量 一致化的基础软件（如操作系统、数 据库等资源），这些基础软件的漏洞 将造成大范围的安全问题与服务隐 患。安全已经成为阻碍万物互联和 云计算发展的最大因素。

边缘计算是万物互联的延伸和 云 计 算 的 扩 展 ，三者 的 有 机 结 合 将 为万物互联时代的信息处理提供较 为完美的软硬件支撑平台，为能源、 交通、制造、医疗等行业带来飞跃式 发展。而通过边缘设备将类似云计 算 的 功 能 带 到 了 网 络 的 边 缘 ，可能 引 入 新 的 安 全 挑 战 ，一些 传 统 的 安 全 解 决 方 法 ，例如 基 于 非 对 称 密 钥 协议和基于网际协议地址（IP）的解 决 方 案 ，无法 有 效 地 应 用 于 边 缘 计 算 系 统 ，进而 带 来 了 一 系 列 全 新 的 安全需求。

同 时 ，边缘计 算 可 以提供 理想 的平台来解决物联网中的许多安全 和 隐 私 问 题 。 在 网 络 边 缘 处 计 算 、 连 接 、存储 能 力 的 协 同 使 用 可 以 达 到 万 物 互 联 应 用 的 部 分 安 全 目 的 。 例 如 ，边缘 设 备 可 以 作 为 加 密 计 算 的 代 理 或 者 在 公 钥 基 础 设 施（PKI） 技 术 中 协 助 认 证 中 心（CA）管 理 证 书 的 发 放 与 撤 销 ，而其 下 面 的 物 联 网设备和传感器就缺乏实现这些操 作的必要资源。

综 上 所述 ，网络边 缘高 度动 态 异构的复杂环境也会使网络难于保 护 ，从而 带 来 新 的 安 全 挑 战 。 边 缘 计 算 同 时 又 为 资 源 、能量 受 限 的 终 端设备提供一套全新的安全解决方 案 。 因 此 ，研究 边 缘 计 算 场 景 的 安 全和隐私保护的相关问题是万物互 联系统得到进一步发展的首要前提

条件。

2.2 边 缘 计 算 安 全 的 需 求 分 析 边 缘 计 算 安 全 需 求 分 析 如 图 2

所示，按照边缘计算参考架构，主要 分为物理安全、网络安全、数据安全 和应用安全 4 个方面的需求。

2.2.1 物 理 安 全 需 求

物 理 安 全 是 保 护 智 能 终 端 设 备 、设施 以 及 其 他 媒 体 避 免 自 然 界 中不可抗力（如地震、火灾、龙卷风、 泥 石 流）及 人 为 操 作 失 误 或 错 误 所 造 成 的 设 备 损 毁 、链路 故 障 等 使 边 缘 计 算 服 务 部 分 或 完 全 中 断 的 情 况。物理安全是整个服务系统的前 提 ，物理 安 全 措 施 是 万 物 互 联 系 统 中必要且基础的工作。

对 于 边缘 计算 设 备来 说，其在 对 外 开 放 的 、不可 控 的 甚 至 人 迹 罕 至 的 地 方 运 行 ，所处 的 环 境 复 杂 多

▲ 图 2 边 缘 计 算 安 全 需 求 分 析

样 ，因此 更 容 易 受 到 自 然 灾 害 的 威 胁 。 且 在 运 行 过 程 中 ，由间 接 或 者 自 身 原 因 导 致 的 安 全 问 题（如 能 源 供应；冷却除尘、设备损耗等），运行 威胁虽然没有自然灾害造成的破坏 彻 底 ，但是 如 果 缺 乏 良 好 的 应 对 手 段，仍然会导致灾难性的后果，使得 边 缘 计 算 的 性 能 下 降 ，服务 中 断 和 数据丢失。

2.2.2 网 络 安 全 需 求

网络安全是指通过采用各种技 术 和 管 理 措 施 ，使网 络 系 统 正 常 运 行，从而确保网络数据的可用性、完 整 性 和 保 密 性 ，以使 系 统 连 续 可 靠 正常地运行，网络服务不中断。

大 数 据处 理背 景 下，海量 终端 设备通过网络层实现与边缘设备的 数 据 交 互 传 输 ，边缘 设 备 可 以 通 过 接入网络层实现更加广泛的互联功 能 。 而 大 量 设 备 的 接 入 ，给网 络 管

2019 年 6 月 第 25 卷 第 3 期

中 兴 通 讯 技 术 Jun. 2019 Vol. 25 No. 3

39

[7]

专 题

万 物 互 联 背 景 下 的 边 缘 计 算 安 全 需 求 与 挑 战

ZTE TECHNOLOGYJOURNAL

马 立 川 等

理 带 来 沉 重 负 担 的 同 时 ，也增 加 了 边 缘 设 备 被 攻 击 的 可 能 性 。 文 献 [5-6] 中 所 采 用 的 攻 击 方 式 大 都 是 在 无 线 传 输 途 中 采 用 窃 听 、截获 数 据 包 等 方 法 进 行 流 量 分 析 ，然后 篡 改或伪造数据包来达到控制目标的 目的。

相 较 于云 计算 数 据中 心，边缘 节 点 的 能 力 有 限 ，更容 易 被 黑 客 攻 击。虽然单个被破坏的边缘节点损 害 并 不 大 ，并且 网 络 有 迅 速 找 到 附 近 可 替 代 节 点 的 调 度 能 力 ；但如 果 黑客将攻陷的边缘节点作为“肉鸡” 去 攻 击 其 他 服 务 器 ，进而 会 对 整 个 网络造成影响。现有大多安全保护 技 术 计 算 保 护 流 程 复 杂 ，不太 适 合 边 缘 计 算 的 场 景 。 所 以 ，设计 适 合 于万物互联背景下边缘计算场景中 轻量级的安全保护技术是网络安全 的重大需求。

2.2.3 数 据 安 全 需 求

数 据 信息 作为 一 种资 源，具有 普 遍 性 、共享性 、增值性 、可处理 性 和 多 效 用 性 ，而数 据 安 全 的 基 本 目 标 就 是 要 确保 数据 的 3 个 安 全 属 性：机密性、完整性和可用性。

要对数据的全生命周期进行管 理 的同 时实现 这 3 个 安全属性才能 保证数据安全。整个生命周期包括 6 个 阶 段 ：创 建 ，数 据 的 产 生 和 采 集过程；存储，数据保存到存储介质 的过程；使用，数据被浏览、处理、搜 索或进行其他操作的过程；共享，数 据在拥有者、合作者、使用者之间交 互的过程；存档，极少使用的数据转 入长期存储的过程；销毁，不再使用 的数据被彻底删除和擦除的过程。

在 边 缘计 算中 ，用户将 数据 外 包 给 边 缘 节 点 ，同时 也 将 数 据 的 控 制 权 移 交 给 边 缘 节 点 ，这便 引 入 了 与 云 计 算 相 同 的 安 全 威 胁 。 首 先 ， 很 难 确 保 数 据 的 机 密 性 和 完 整 性 ， 因为外包数据可能会丢失或被错误 地 修 改 。 其 次 ，未经 授 权 的 各 方 可 能 会 滥 用 上 传 的 数 据 图 谋 其 他 利 益。虽然相对于云来说边缘计算已 经 规 避 了 多 跳 路 由 的 长 距 离 传 输 ， 很 大 程 度 地 降 低 了 外 包 风 险 ；但是 边缘计算设备部署的应用属于不同 的 应 用 服 务 商 ，接入 网 络 属 于 不 同 的 运 营 商 ，导致 边 缘 计 算 中 多 安 全 域 共 存 、多种 格 式 数 据 并 存 。 因 此 属于边缘计算的数据安全问题也日 益 突 出 ，如在 一 个 边 缘 节 点 为 多 个 用 户 服 务 时 ，如何 确 保 用 户 数 据 的 安全隔离？在如此复杂多变的环境 中，一个边缘节点瘫痪后，如何实现 安全快速地迁移数据？当多个边缘 节 点 协 同 服 务 时 ，如何 能 够 在 不 泄 露各自数据的情况下设计多方的协 作服务？

另一个万物互联背景下边缘计 算的数据安全需求就是用户隐私保 护。比起云中心隐私数据泄露的风 险 ，边缘 计 算 设 备 位 于 靠 近 数 据 源 的 网 络 边 缘 侧 ，相对 于 位 于 核 心 网 络 中 的 云 计 算 数 据 中 心 ，可以 收 集 更 多 用 户 高 价 值 的 的 敏 感 信 息 ，包 括位置信息、生活习惯、社交关系甚 至 健 康 状 况 等 ，边缘 计 算 是 否 会 成 为商业公司收集用户隐私数据的平 台？物联网设备的计算资源难以执 行 复 杂 的 隐 私 保 护 算 法 ，边缘 式 大 数据分析中如何在数据共享时保证 用户的隐私？这些问题都将成为边

缘计算发展的重要阻碍。

2.2.4 应 用 安 全 需 求

应 用 安全 ，顾名思 义就 是保 障 应 用 程 序 使 用 过 程 和 结 果 的 安 全 。 边 缘 式 大 数 据 处 理 时 代 ，通过 将 越 来越多的应用服务从云计算中心迁 移 到 网 络 边 缘 节 点 ，能保 证 应 用 得 到 较 短 的 响 应 时 间 和 较 高 的 可 靠 性 ，同时 大 大 节 省 网 络 传 输 带 宽 和 智能终端电能的消耗。但边缘计算 不仅存在信息系统普遍存在的共性 应用安全问题，如拒绝服务攻击、越 权 访 问 、软件漏 洞 、权限滥 用 、身份 假 冒 等 ，还由 于 其 自 身 特 性 存 在 其 他的应用安全的需求。在边缘这种 多 安 全 域 和 接 入 网 络 共 存 的 场 景 下，为保证应用安全，该如何对用户 身份进行管理和实现资源的授权访 问 则 变 得 非 常 重 要 。 身 份 认 证 、访 问控制和入侵检测相关技术便是在 边缘计算环境下保证应用安全的重 点需求。

3 边 缘 计 算 安 全 挑 战

通过对边缘计算安全需求的讨 论 分 析 可 以 看 出 ：边缘 计 算 的 特 性 使其在构建安全保护方案时给系统 开发人员带来了重大挑战。

3.1 身 份 认 证

身 份认 证，也称“身 份验 证”或 “ 身 份 鉴 别 ”，是验证或 确 定 用 户 提 供的访问凭证是否有效的过程。用 户可以是个人、应用或服务，所有的 用 户 都 应 在 被 认 证 后 才 能 访 问 资 源 ，从而 确 定 该 用 户 是 否 具 有 对 某 种 资 源 的 访 问 和 使 用 权 限 ，使系 统

40

中 兴 通 讯 技 术

2019 年 6 月 第 25 卷 第 3 期

Jun. 2019 Vol. 25 No. 3

[8]

[9]

马 立 川 等

万 物 互 联 背 景 下 的 边 缘 计 算 安 全 需 求 与 挑 战

ZTE TECHNOLOGYJOURNAL

专 题

的访问策略能够可靠、有效地执行， 防止攻击者假冒合法用户获得资源 的 访 问 权 限 ，保证 系 统 和 数 据 的 安 全，以及授权访问者的合法利益。

在 边 缘计 算中 ，不同可 信域 中 的 边 缘 服 务 器 、云服 务 提 供 商 和 用 户 分 别 提 供 和 访 问 实 时 服 务 ，其分 散 化 、实时 服 务 的 低 延 迟 需 求 和 用 户的移动性给身份认证的实现带来 了 巨 大 的 障 碍 ，很难 保 证 所 有 涉 及 的实体都是可信的。在访问这些服 务 之 前 ，应该 对 每 个 用 户 进 行 身 份 验 证 ，以 确 保 其真 实 性和 可 信 性。 身 份 认 证 应 具 备 的 功 能 包 括 ：一方 面 应 能 够 在 分 布 式 异 构 网 络 环 境 下，使用相关的协议、规范以及技术 将 分 散 的 身 份 信 息 进 行 集 中 管 理 ， 实 现 单 点 登 录 ，也可 以 方 便 地 扩 充 跨 身 份 标 识 域 的 访 问 等 功 能 ；另一 方 面 应 提 供 友 好 的 体 验 环 境 ，保护 用 户 隐 私 ，有效 地 对 用 户 的 行 为 进 行审计。

身份认证是终端设备安全的基 本 要 求 ，许多 万 物 互 联 设 备 没 有 足 够的内存和中央处理器（CPU）功率 来 执 行 认 证 协 议 所 需 的 加 密 操 作 。 这些资源有限的设备可以将复杂的 计算和存储外包给可以执行认证协 议 的 边 缘 设 备 ，与此 同 时 也 会 带 来 一 定 的 问 题 ：终端 用 户 和 边 缘 计 算 服 务 器 之 间 必 须 相 互 认 证 ，这种 多 安全域共存的情况下安全凭证从何 而来？如何在大量分布式边缘服务 器和云计算中心之间实现统一的身 份认证和密钥管理机制？万物互联 中 存 在 大 量 的 资 源 受 限 设 备 ，无法 利用传统的 PKI 体 制对 边缘计算设 备或服务进行认证。边缘计算环境

下 终 端 具 有 很 强 的 移 动 性 ，如何 实 现用户在不同边缘设备切换时的高 效 认 证 具 有 很 大 挑 战 。 显 然 ，轻 量级的身份认证技术是保证边缘计 算安全的前提和挑战。

3.2 访 问 控 制

访问控制是基于预定模式和策 略对资源的访问过程进行实时控制 的 技 术 ，按用 户 身 份 及 其 所 归 属 的 某项定义组来限制用户对某些信息 项 的 访 问 ，或限 制 对 某 些 控 制 功 能 的使用。访问控制的任务是在满足 用户最大限度享受资源共享需求的 基 础 上 ，实现 对 用 户 访 问 权 限 的 管 理，防止信息被非授权篡改和滥用， 是 保 证 系 统 安 全 、保护 用 户 隐 私 的 可 靠 工 具 。 在 万 物 互 的 联 背 景 下 ， 需要访问控制以确保只有受信任方 才 能 执 行 给 定 的 操 作 ，不同 用 户 或 终端设备具有访问每个服务的独特 权限。

访问控制除了负责对资源访问 控 制 外 ，还要 对 访 问 策 略 的 执 行 过 程 进 行 追 踪 审 计 。 在 边 缘 计 算 中 ， 访 问 控 制 变 得 更 加 艰 难 ，主要 原 因 在 于 ：首先 要 求 边 缘 计 算 服 务 提 供 商能够在多用户接入环境下提供访 问控制功能；其次，访问控制应支持 用户基本信息和策略信息的远程提 供 ，还应 支 持 访 问 控 制 信 息 的 定 期 更新；最后，对于高分布式且动态异 构数据的访问控制本身就是一个重 要的挑战。

3.3 入 侵 检 测

入侵检测通过包括监测、分析、 响 应 和 协 同 等 一 系 列 功 能 ，能够 发

现系统内未授权的网络行为或异常 现 象 ，收集 违 反 安 全 策 略 的 行 为 并 进行统计汇总，从而支持安全审计、 进 攻 识 别 、分析 和 统 一 安 全 管 理 决 策 。 从 企 业 角 度 看 ，任何 试 图 破 坏 信 息 及 信 息 系 统 完 整 性 、机密 性 的 网络活动都被视为入侵行为。入侵 检 测 技 术 广 泛 应 用 于 云 系 统 中 ，以 减 轻 内部 攻 击 、泛 洪 攻 击、端 口 扫 描、虚拟机攻击和 hypervisor 攻 击等 入侵行为。

在 边 缘计 算中 ，外部和 内部 攻 击者可以随时攻击任何实体。若没 有实施适当的入侵检测机制来发现 终端设备和边缘节点的恶意行为或 协议违规，则会逐步破坏服务设施， 进而影响整个网络。

但是，在万物互联环境下，由于 设 备 结构 、协 议 、服 务 提 供 商的 不 同 ，难 以 检 测 内 部 和 外 部 攻 击 。 此 外 ，如何 通 过 资 源 能 力 受 限 的 边 缘设备间的系统来进行全局的入侵 检测，使其能够在大规模、广泛地理 分 布 和 高 度 移 动 的 环 境 中 得 到 应 用，具有十分重要的意义。

3.4 隐 私 保 护

万物互联系统的目标是通过收 集海量数据为用户提供多种个性化 服 务 。 由 于 终 端 设 备 资 源 受 限 ，缺 乏 对 数 据 加 密 或 解 密 的 能 力 ，这使 得它容易受到攻击者的攻击。

边缘计算将计算迁移到临近用 户 的 一 端 ，直接 对 数 据 进 行 本 地 处 理、决策，在一定程度上避免了数据 在 网 络 中 长 距 离 的 传 播 ，降低 了 隐 私 泄 露 的 风 险 。 然 而 ，由于 边 缘 设 备 获 取 的 用 户 第 一 手 数 据 ，能够 获

2019 年 6 月 第 25 卷 第 3 期

中 兴 通 讯 技 术 Jun. 2019 Vol. 25 No. 3

41



作 者 简 介

马 立 川 ，西安 电 子 科 技 大 学 网 络 与 信 息 安 全 学 院 师 资 博 士 后 ；主要 研 究 方 向 为 隐 私 保 护 、边缘计 算 安 全 等 。

裴 庆 祺 ，西安 电 子 科 技 大 学 教 授 、博士生 导 师 、综合业 务 网 理 论 与 关 键 技 术 国 家 重 点 实 验 室（ISN）成 员 、区块 链 应 用 与 评 测 研 究 中 心 主 任 ， 西 安 市 移 动 边 缘 计 算 及 安 全 重 点 实 验 室 主 任 ，陕西 省 区 块 链 与 安 全 计 算 重 点 实 验 室 执 行 主 任 ；主要 研 究 方 向 为 认 知 网 络 与 数 据 安 全 、区块

链 、边缘计 算 及 安 全 等 领 域 。

肖 慧 子 ，西安 电 子 科 技 大 学 通 信 工 程 学 院 在 读 博 士 研 究 生 ；主要 研 究 方 向 为 边 缘 计 算 和 物 联 网 中 的 安 全 与 隐 私 问 题 。



专 题

万 物 互 联 背 景 下 的 边 缘 计 算 安 全 需 求 与 挑 战

ZTE TECHNOLOGYJOURNAL

马 立 川 等

得大量的敏感隐私数据。如何能够 保证用户在使用服务的同时又不泄 露其敏感信息对边缘计算中的隐私 保护算法提出了更高的要求。

3.5 密 钥 管 理

密钥管理包括从密钥产生到密 钥 销 毁 的 各 个 方 面 ，主要 表 现 于 管 理体制、管理协议和密钥的产生、分 配 、更换和 注 入 等 ，包含密 钥 生 成 、 密 钥 分 发 、验证密 钥 、更新 密 钥 、密 钥 存 储 、备份密 钥 、密钥的 有 效 期 、 销毁密钥这一系列的流程。密钥在 已 授 权 的 加 密 模 块 中 生 成 ，高质 量 的 密 钥 对 于 安 全 是 至 关 重 要 的 ，整 个密码系统的安全性并不取决于密 码 算 法 的 机 密 性 ，而是 取 决 于 密 钥 的 机 密 性 。 一 旦 密 钥 遭 受 泄 露 、窃 取、破坏，机密信息对于攻击者来说 已 经 失 去 保 密 性 。 由 此 可 见 ，密钥 管理对于设计和实施密码系统而言 至关重要。

在 万 物互 联环 境 中，由于 云服 务 商 、边缘 服 务 商 和 用 户 对 密 钥 管 理系统与信息技术（IT）基础设施具 有 不 同 的 所 有 权 和 控 制 权 ，这使 得 面向边缘计算环境的密钥管理比传 统 信 息 系 统 的 密 钥 管 理 更 为 复 杂 。 因为每个应用出于特定的安全目的 管 理 其 安 全 密 钥 ，使得 跨 应 用 密 钥 管 理 变 得 尤 为 复 杂 ，参与 多 个 应 用 程序的用户设备需要管理多个安全 密 钥 或 口 令 ，增加 了 密 钥 泄 露 的 风 险 并 危 及 服 务 的 安 全 性 。 显 然 ，在 大 规 模 、异构、动态 的 边 缘 网 络 中 ， 保 证 用 户 和 用 户 之 间 、用户 和 边 缘 设 备 之 间 、边缘 设 备 和 边 缘 设 备 之 间 、边缘 设 备 和 云 服 务 器 之 间 的 信

息 交 互 安 全 ，给边 缘 计 算 模 式 下 实 现高效的密钥管理方案带来了严峻 的挑战。

4 结 束 语

随 着 万物 互联 时 代的 到来 ，基 于云计算模型的集中式大数据处理 模式已经无法满足网络边缘设备所 产 生 海 量 数 据 处 理 的 实 时 性 、安全 性 和 低 能 耗 等 需 求 。 为 此 ，将原 有 云计算中心的部分或者全部计算任 务 迁 移 到 数 据 源 的 附 近 执 行 ，边缘 计算在梯联网、工业机器人、无人驾 驶 、智慧 交 通 等 领 域 扮 演 着 越 来 越 重要的角色。作为一种新型的去中 心化架构，它将云计算的存储、计算 和 网 络 资 源 扩 展 到 网 络 边 缘 ，以支 持大规模的协同万物互联应用。然 而 ，由于 边 缘 设 备 更 加 靠 近 网 络 边 缘侧，网络环境更加复杂，并且边缘 设 备 对 于 终 端 具 有 较 高 的 控 制 权 限 ，导致 其 在 提 高 万 物 互 联 网 络 中 数 据 传 输 和 处 理 效 率 的 同 时 ，不可 避 免 地 带 来 一 些 新 的 安 全 威 胁 ，如 物 理 安 全 、网络安 全 、数据 安 全 、应 用 安 全 等 。 同 时 ，边缘 计 算 模 式 也 给 身 份 认 证 、访问控 制 、入侵检 测 、 隐 私 保 护 、密钥 管 理 等 方 面 带 来 了 严 峻 的 挑 战 。 为 此 ，我们 需 要 清 晰 地认识边缘计算安全框架和业务流 程，设计安全的边缘计算架构，这些 对于促进边缘计算的进一步普及和 发展具有十分重要的意义。

参 考 文 献

[1] 施 巍 松 , 孙 辉 , 曹 杰 , 等 . 边 缘 计 算 : 万 物 互 联 时 代 新 型 计 算 模 型 [J]. 计 算 机 研 究 与 发 展 , 2017,

54(5): 907-924. DOI:10.7544/issn1000-

1239.2017.20160941

[2] 施 巍 松 , 刘 芳 , 孙 辉 , 等 . 边 缘 计 算 [M]. 北 京 ：科 学 出 版 社 . 2018

[3] 边 缘 计 算 产 业 联 盟 , 工 业 互 联 网 产 业 联 盟 . 边 缘 计 算 与 云 计 算 系 统 白 皮 书 [R]. 2018

[4] HE D J, CHAN S, GUIZANI M. Security in the Internet of Things Supported by Mobile Edge Computing [J]. IEEE Communications Magazine, 2018, 56(8): 56-61. DOI:10.1109/ mcom.2018.1701132

[5] KOSCHER K, CZESKIS A, ROESNER F, et al. Experimental Security Analysis of a Modern Automobile[C]//2010 IEEE Symposium on Security and Privacy. USA: IEEE, 2010: 447- 462. DOI:10.1109/SP.2010.34

[6] 云 计 算 白 皮 书 [EB/OL]. [2018-12-20]. http:// www.199it.com/archives/764250.html

[7] 卿 昱 . 云 计 算 安 全 技 术 [M]. 北 京 : 国 防 工 业 出 版 社 , 2016:53-54

[8] HE D B, ZEADALLY S, WU L B, et al. Analysis of Handover Authentication Protocols for Mobile Wireless Networks Using Identity- Based Public Key Cryptography [J]. Computer Networks, 2017, 128: 154-163. DOI:10.1016/j. comnet.2016.12.013

[9] PRABAVATHY S, SUNDARAKANTHAM K, SHALINIE S M. Design of Cognitive Fog Computing for Intrusion Detection in Internet of Things[J]. Journal of Communications and Networks, 2018, 20(3): 291-298. DOI:10.1109/ jcn.2018.000041

42

中 兴 通 讯 技 术

2019 年 6 月 第 25 卷 第 3 期

Jun. 2019 Vol. 25 No. 3