第 39 卷 第 5 期
2024 年 10 月

天津科技大学学报
Journal of Tianjin University of Science & Technology

Vol. 39 No. 5
Oct. 2024

DOI:10.13364/j.issn.1672-6510.20230224
数字出版日期：2024–06–21；数字出版网址：http://link.cnki.net/urlid/12.1355.n.20240620.1521.005

边缘计算环境下基于零信任的数字信誉评分模型设计

许佳文，王 聪，熊昱雯，张翼英
（天津科技大学人工智能学院，天津 300457）

摘 要：边缘计算通过在接近数据源的地方进行实时处理，与云计算相结合，提供高效能、低延迟的计算解决方案，构建了全面的分布式计算体系。然而，边缘计算的分布式和内部信任特性也导致了边界安全模糊的问题。零信任架构的出现打破了原先静态的边界防御模式，使设备在网络中能实现动态安全。但是，边缘设备的分布式特性导致边缘计算在零信任架构中存在动态管理的复杂性、资源限制等困难。针对此问题，本文提出一种基于零信任的数字信誉评分模型（DRSM），通过结合区块链，实现边缘计算环境下的动态访问管理和授权。该方案有助于解决边界安全模糊的问题，降低恶意攻击对系统造成的影响。仿真结果表明，本文模型能够有效减少异常边缘设备的访问，提高系统的安全性。

关键词：边缘计算；零信任；信誉管理模型
中图分类号：TP393.08 **文献标志码**：A **文章编号**：1672-6510（2024）05-0072-09

Design of Digital Reputation Scoring Model Based on Zero Trust in Edge Computing Environment

XU Jiawen，WANG Cong，XIONG Yuwen，ZHANG Yiying
（College of Artificial Intelligence，Tianjin University of Science & Technology，Tianjin 300457，China）

Abstract：Edge computing combines real-time processing near the data source with cloud computing to provide high-efficiency and low-latency computing solutions and build a comprehensive distributed computing system. However，the distributed and internal trust characteristics of edge computing also lead to the problem of fuzzy boundary security. The appearance of zero-trust architecture breaks the original static boundary defense mode and makes the device realize dynamic security in the network. The distributed nature of edge devices however leads to the difficulties of dynamic management in zero-trust architecture，such as complexity and resource limitation. To solve this problem，in this article we propose a digital reputation scoring model（DRSM）based on zero trust，which combines with blockchain to realize dynamic access management and authorization in edge computing environment. This scheme is helpful to solve the problem of fuzzy boundary security and reduce the impact of malicious attacks on the system. The simulation results showed that the proposed model could effectively reduce the access of abnormal edge devices and improve the security of the system.

Key words：edge computing；zero trust；reputation management model

引文格式：
许佳文，王聪，熊昱雯，等. 边缘计算环境下基于零信任的数字信誉评分模型设计[J]. 天津科技大学学报，2024，39（5）：72–80.
XU J W，WANG C，XIONG Y W，et al. Design of digital reputation scoring model based on zero trust in edge computing environment[J]. Journal of Tianjin university of science & technology，2024，39（5）：72–80.

边缘计算是物联网（IoT）的分布式计算模型，旨在使数据处理和计算功能更接近数据源的边缘设备（例如传感器、智能手机、物联网设备），而不是传统的集中式云计算数据中心[1]。边缘计算的网络体系结

收稿日期：2023–11–30；**修回日期**：2024–04–22
作者简介：许佳文（1998—），男，江苏南京人，硕士研究生；**通信作者**：王 聪，副教授，wangcongjcdd@tust.edu.cn

构通常基于边界防御和内部信任的概念。它将网络划分为内部网络和外部网络，内部网络被认为是相对可信任的区域，外部网络被认为是不可信任区域[2]。边缘计算的分布式和开放式的结构，导致网络边界模糊和边界信任不可靠，拥有过高权限的网络可能会对内部安全构成威胁[3]。当今的网络系统通常采用固定权限模型。该模型要求用户一旦被授予某一特权，他们就会保留该特权直到被撤销或修改。然而，这种静态权限模型使其难以适应用户权限和动态要求的变化。此外，边缘计算具有的分布式和开放式的特点，使它很容易受到网络嗅探、中间人攻击、分布式拒绝服务等攻击[4–5]。为了有效地解决这些问题，必须开发和使用新的技术。

作为无边界趋势下网络安全问题的解决方案，零信任概念应运而生[6]。零信任网络通过采用不信任任何用户、设备或应用程序并强制进行身份验证和授权的方法，确保只有授权的用户和设备才能访问资源。这种架构有效地限制了攻击者的能力，降低潜在的安全风险，并提供了更强的隐私保护机制。

为了成功地将零信任架构应用于边缘计算，本研究通过边缘计算模型中边缘设备和边缘服务器的动态控制实现边缘设备的动态授权。在边缘计算的动态控制过程中，对边缘设备和边缘服务器进行实时信誉管理，确保其在“始终认证、永不信任”的原则下运行。这些举措有助于增强边缘计算场景中系统的安全性和隐私性，并有助于解决内部安全问题。

Sandal 等[7]提出一种基于信誉的攻击者识别策略，根据信誉指数将用户分为诚实、可疑和恶意 3 种状态并进行管理。Deng 等[8]提出一种基于信誉的边缘计算网络信任评估和管理系统，以提高其安全性和效率，但在研究中并没有分析如何防止恶意节点伪造或篡改身份。Liao 等[9]为支持边缘计算的物联网系统提出基于信誉和投票的区块链共识机制，但研究中未详细阐述如何应对网关节点可能成为系统中单点故障的问题。Huang 等[10]提出一种基于边缘计算的车载网络的分布式信誉管理模型（distributed reputation model，DRM），该模型使用多种主观逻辑提高信誉更新的准确性。但是，该模型没有考虑车辆的隐私保护和声誉激励机制，只是依赖于地方当局的可信度和服务提供商的信誉进行辅助优化。这可能导致车辆的信誉信息被泄露或滥用，且削弱了车辆维护信誉的动力。Yuan 等[11]提出一种针对物联网边缘设备的可靠轻量级信任计算机制（reliable and lightweight trust computing mechanism，RLTM），通过全局信任计算抵御恶意反馈提供者造成的诽谤攻击。该研究假设只有恶意节点会发动网络攻击。然而，在实际的物联网边缘计算环境下，众多不同类型的攻击者可能会根据自己的利益或环境的变化而调整相应的策略，有时候提供虚假的反馈或服务，逃避信任机制的检测和惩罚。现在，越来越多的研究人员在不同模型中应用零信任网络，以应对日益脆弱的安全边界环境。Lukaseder 等[12]提出基于身份和信任的网络模型，并使用该模型应对校园网络中的安全威胁和挑战。Guo 等[13]重构了零信任系统基本框架的内部结构，引入冗余机制实现内生安全增益。Mehraj 等[14]提出云计算中基于信任的授权系统概念零信任模型。不过该研究并没有提供零信任模型的具体设计细节和实现方法。Li 等[15]提出一种基于数字身份的分布式动态认证方案，确保边缘计算中安全事件的可追溯性。不过该研究没有详细说明如何保护数字身份的隐私和安全。

这些解决方案在不同的环境、框架和应用程序中有所不同。在边缘计算环境下建立动态信任模型是一项多维任务，当前研究没有提供实现边缘计算零信任的具体解决方案。现有的信任管理机制在应用于边缘计算时，往往严重依赖中心化存储和第三方参与，效率低下，容易出现单点故障，从而带来过多的安全问题[16]。

为了应对这些挑战，本文提出一种基于区块链的零信任架构，支持对边缘服务器的有效控制，并实现边缘计算环境下边缘设备的分布式动态访问和授权。基于此零信任架构，本文设计了数字信誉评分模型（digital reputation scoring model，DRSM）。DRSM 通过零信任组件策略引擎和信任引擎有效管理边缘服务器和边缘设备的数字身份，增强边缘服务器的可靠性以及边缘设备与边缘服务器交互过程中的安全性和隐私性。

1　系统模型概述

1.1　系统模型

在边缘计算环境下，本文利用零信任架构并结合数字身份和区块链技术，改善边缘设备和服务器之间访问的安全问题。数字身份是区块链和零信任的重要组成部分，它通过分布式账本技术记录边缘设备的身份信息。零信任架构包括 3 个关键组件：网络代

理、策略引擎和信任引擎[17]。网络代理由数字身份、数字身份评分以及时间戳构成。策略引擎发布数字身份评分策略并处理来自网络代理的授权请求。根据这些策略和请求，策略引擎决定是否允许网络代理访问某些资源或服务。信任引擎的职责是对边缘设备网络请求的风险进行数值评估。系统模型如图 1 所示。

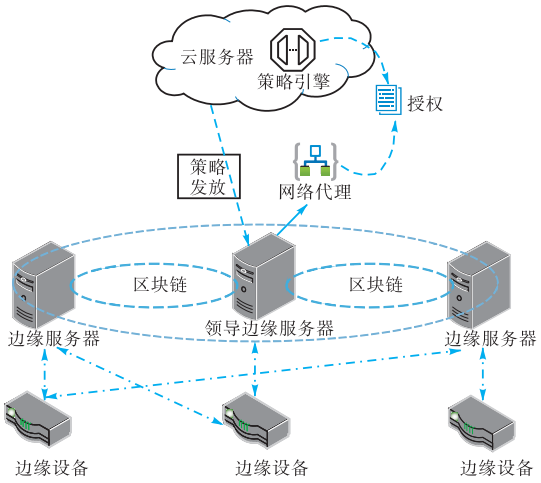


图 1　系统模型

Fig. 1　System model

系统模型由云服务器(cloud server，CS)、边缘服务器(edge server，ES)、边缘设备(edge device，ED)、策略引擎(policy engine，PE)、信任引擎(trust engine，TE)和部署在边缘服务器节点上的区块链网络组成。边缘服务器负责其区域内边缘设备的注册、认证和数字身份生成。多个边缘服务器组成一组，根据信誉评分的实用拜占庭容错协议(T-PBFT)共识算法[18]计算出每个 ES 节点的信誉评分，并选举出领导边缘服务器(leader ES，LES)。策略引擎部署在云服务器上，它负责生成动态数字身份信誉评分策略，并将评分策略发送给领导边缘服务器。领导边缘服务器接收评分策略并通过智能合约发送给其他边缘服务器，部署在边缘服务器上的信任引擎负责计算边缘设备数字身份的直接信誉值，接着领导边缘服务器上的信任引擎负责计算最终信誉评分并组成网络代理，最后领导边缘服务器将网络代理发送给云服务器上的策略引擎进行授权。

1.2　EigenTrust 模型

EigenTrust 模型[19]是最权威的信誉管理模型之一，可以应用于点对点(peer-to-peer，P2P)网络环境。EigenTrust 模型根据其他节点与自身节点请求的一致性，计算并排序网络中每个节点的信誉值。

EigenTrust 模型通过计算节点的直接信誉值、间接信誉值，最后得出节点的全局信誉值。

1.2.1　直接信誉值

每个节点a可以存储它与节点 b 进行的满意交易的数量 $N_{\mathrm{sat}}(a,b)$，以及它与节点 b 进行的不满意交易的数量 $N_{\mathrm{unsat}}(a,b)$。那么，本地信誉值 S_{ab} 可以定义为

$$S_{ab}=N_{\mathrm{sat}}(a,b)-N_{\mathrm{unsat}}(a,b) \tag{1}$$

经过一定数量的交易后，从节点 a 到节点 b 的直接信誉值 C_{ab} 可以定义为

$$C_{ab}=\frac{\max(S_{ab},0)}{\sum_{b}\max(S_{ab},0)} \tag{2}$$

1.2.2　间接信誉值

间接信誉值是某个节点对其他节点推荐信息的可信度，它建立在信任传递的基础上，间接信誉值与直接信誉值相关。例如，无直接交易关系的节点 a 和节点 d 的间接信誉值 C_{ad} 被定义为

$$C_{ad}=\sum_{k}C_{ak}C_{kd} \tag{3}$$

式中：k 为节点 a 和节点 d 之间有交易关系的所有节点。

1.2.3　全局信誉值

通过节点间的交易记录计算每个节点的全局信誉值 T_i，计算公式为

$$T_i=C_{1i}T_1+\cdots+C_{ri}T_i+\cdots+C_{\omega i}T_{\omega} \tag{4}$$

式中：C_{ri} 为节点 r 对节点 i 的直接或间接信誉值，ω 为网络中节点总数，i 的取值范围为 $[1,\omega]$。

1.3　边缘设备的动态访问

当数字身份上传到区块链网络后，信任引擎便会对数字身份进行信誉评分。策略引擎根据评分动态授权网络代理，从而实现零信任网络中边缘计算的动态控制和授权。边缘设备动态访问流程如图 2 所示。图 2 左栏描述了边缘设备数字身份上链，图 2 右栏描述了基于边缘设备数字身份信誉评估的网络代理授权过程。

1.3.1　边缘设备数字身份上链

边缘服务器对边缘设备进行初始身份验证。如果认证成功，边缘服务器根据边缘设备的身份信息(当前设备位置、IP 地址、设备序列号、用户配置等)生成边缘设备数字身份(digital identify，DID)，之后边缘服务器对边缘设备进行连续认证。如果多次认证失败，边缘服务器会拒绝边缘设备的访问请求。另外，边缘服务器创建连接请求消息 Tx_link，Tx_link 包含边缘设备的公钥信息(public key，PK)和 DID。

边缘服务器将 Tx_link 添加到本地数据库，用于后续的连接和交互过程。一旦区块链网络启动并运行，边缘服务器就会将 Tx_link 提交到待处理交易池中。边缘设备等待部署在边缘服务器上的区块链节点完成基于 EigenTrust 模型的 T-PBFT 共识过程。如果没通过验证，将进行领导边缘服务器节点的重新选举；如果通过验证，区块链节点将创建一个包含数字身份信息的新块，这表示边缘设备的数字身份信息已经成功上传。

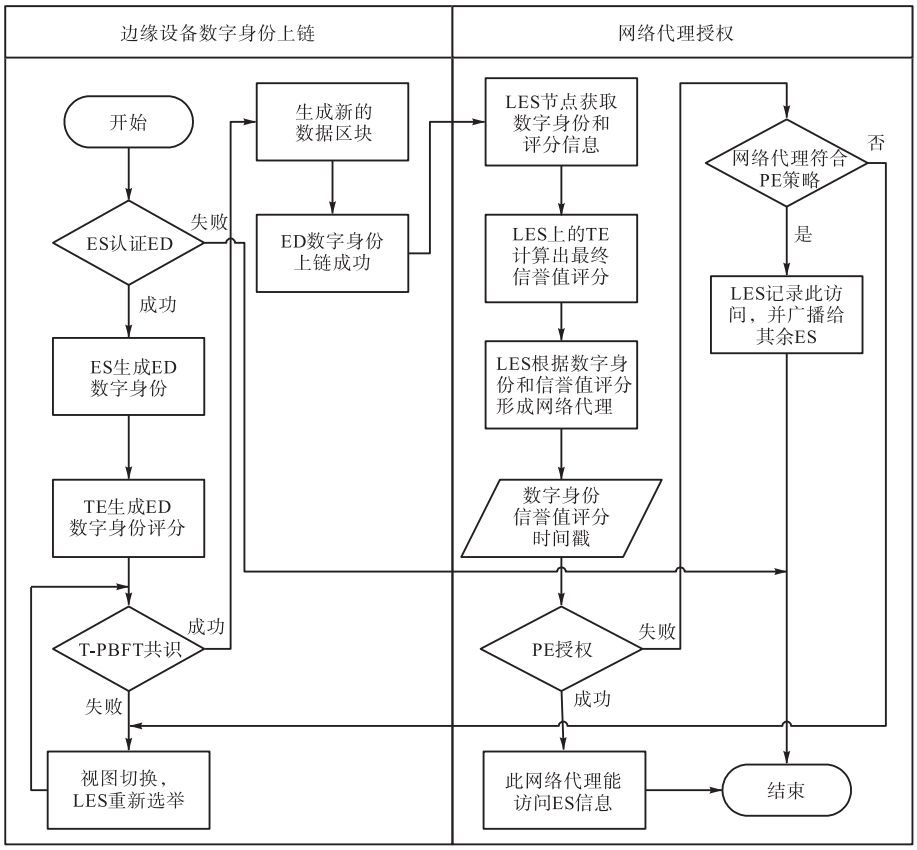


图 2　边缘设备动态访问流程

Fig. 2　Dynamic access process of ED

1.3.2　网络代理授权

通过基于 EigenTrust 模型的 T-PBFT 共识算法，每个边缘服务器都会有一个信誉评分。领导边缘服务器通过智能合约获得边缘设备数字身份的评分以及该边缘服务器的信誉评分。领导边缘服务器上的信任引擎通过边缘设备数字身份中包含的信息计算历史信誉评分，并结合激励功能计算出边缘设备数字身份的最终信誉值。

根据策略引擎的策略，领导边缘服务器生成网络代理并提交策略引擎进行授权。如果授权成功，边缘设备可以使用该网络代理访问边缘服务器资源。如果授权失败，策略引擎会检查创建的网络代理是否符合策略要求。如果符合要求，领导边缘服务器会记录访问并将此边缘设备数字身份信息广播给其他边缘服务器。如果网络代理不符合策略要求，则会进行视图切换并重新选举领导边缘服务器。

2　信誉评分模型

2.1　DRSM 的组成部分

在 DRSM 中，边缘服务器和边缘设备数字身份的信誉评分从 0 到 1 变化，分数越高表明系统的信任程度越高。DRSM 通过对边缘服务器和边缘设备的数字身份信誉进行动态评分，实现边缘设备的动态访问，保证整个系统实时处于相对安全的状态。DRSM 如图 3 所示，它包含边缘设备数字身份推荐信誉评分（recommend score of DID，RED）模块、历史信誉评分（historical reputation score，HRS）模块、激励信誉评分（incentive reputation score，IRS）模块，以及这 3 个模块加权相加得到的边缘设备数字身份最终信誉值

(final reputation score of DID, FRS)模块。

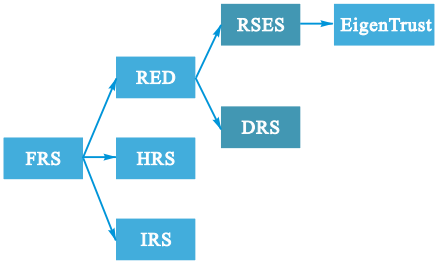


图 3　数字信誉评分模型

Fig. 3　Digital reputation scoring model

RED：RED 由边缘服务器的信誉评分 RESE (reputation score of ES, RESE)和边缘设备的数字身份直接信誉评分(digital reputation score, DRS)组成。DRSM 模型认为边缘计算的关键组成部分即边缘服务器和边缘设备都是不可信的。由于信任引擎部署在边缘服务器上并对边缘设备进行直接评分，因此 RSES 和 DRS 将被一起评估，以符合“零信任”策略。RSES 和 DRS 的综合信誉评分反映了边缘设备在系统中最初的信誉。

HRS：每当边缘设备在历史上与系统交互时，领导边缘服务器上的信任引擎都会记录 FRS，并以此计算 HRS。这样可以鼓励边缘设备每次连接都做正确的事情，以此提高它们的整体信誉评分。

IRS：IRS 体现了对边缘设备遵守策略引擎规则的激励，即边缘设备数字身份可以获得更快的信誉增长，这使边缘设备更容易获取边缘服务器资源。

当边缘设备想要访问边缘服务器的资源时，必须通过某个边缘服务器的认证，然后边缘服务器生成边缘设备的数字身份并对该数字身份进行评估。在 DRSM 中，RED 由边缘服务器和边缘设备的行为决定。RSES 考虑了其在共识过程中的行为。DRS 衡量了边缘设备是否向边缘服务器发送合规的个人信息。边缘服务器在访问同一区域内的任意边缘服务器时，边缘服务器都会记录信誉评分，据此形成该边缘设备的 HRS。此外，通过设置 IRS，表现良好的边缘设备可以获得更高的信誉评分，可以优先访问边缘服务器资源。RED、HRS 和 IRS 加权相加得到 FRS，FRS 随着时间的推移更新以保证其时效性。

2.2　信誉值计算

2.2.1　RED 的计算

(1) RSES 的计算

边缘设备数字身份的信誉评分由部署在边缘服务器上的策略引擎计算，因此边缘服务器的信誉对边缘设备数字身份信誉值的评估也起着相当重要的作用。ES 节点面对边缘设备的数字身份上链请求，运用基于 EigenTrust 模型的 T-PBFT 算法进行共识过程，共识过程中通过 EigenTrust 模型对每个 ES 节点的信誉值进行计算与排序。传统的 T-PBFT 算法认为每个 ES 节点都是平等的，但边缘计算环境下每个节点的基本配置在通信半径、安全性、网络带宽等方面存在差异。因此，基于EigenTrust 模型，对所有节点进行评分[14]。初始选举时，主节点编号 P 按式(5)选举。

$$P = v \bmod N \tag{5}$$

式中：v 为视图数，N 为系统中 ES 节点数。

在出现一轮共识过程已经完成、主节点无法完成共识(作为恶意节点或故障节点)、主节点形成的网络代理不满足策略引擎的要求这 3 种情况时，区块链系统将进行视图切换，将 v 的个数加 1，用于 LES 节点的重选。

$$P = v \mod (N - m) \tag{6}$$

基于由策略引擎制定的策略，只有具有较高信誉值的 $(N-m)$ 个节点才可以被选择作为共识组节点参与下一轮共识过程，而具有较低信誉值的 m 个节点则被排除在共识过程之外。

ES 节点作为对等网络中的节点，每个节点向其他节点发送请求，然后等待其他节点回复。在每一轮的 T-PBFT 过程中使用 EigenTrust 模型计算第 i 个 ES 节点的信誉评分 RSES 为 R_i，即

$$R_i = T_i \tag{7}$$

(2) DRS 的计算

边缘服务器认证申请连接的边缘设备，并记录设备的数量和通过认证的数量。边缘服务器向经过认证的边缘设备发放数字身份。根据领导边缘服务器发送的策略引擎制定的评分策略，部署在边缘服务器上的信任引擎对认证边缘设备的数字身份信息进行信誉评分。获取第 j 个 ES 对第 i 个 ED 的初始数字身份信誉评分 DRS。

信任引擎基于数字身份信息与策略引擎制定的访问要求的一致性和连续认证的正确性对边缘设备数字身份的信誉分数进行评分。

策略引擎定义数字身份中包含的需要评分的信息为 K_g, $g=1,2,\cdots,n$，策略引擎为每一项 K 设置一个权重 φ_g, $g=1,2,\cdots,n$，并为连续认证评分设置权重 φ_{n+1}，$\varphi_1+\cdots+\varphi_n+\varphi_{n+1}=1$。每个 K 的评分 e 的分值范围为[−1, 1]。字典 D 将 K 对应的评分关系表示为

$$D=\{K_1:e_1, K_2:e_2, \cdots, K_n:e_n\} \tag{8}$$

边缘服务器根据策略引擎的策略对数字身份进行直接评分，即

$$E=\sum_{1}^{n}e_g\varphi_g, g=1,2,\cdots,n \tag{9}$$

策略引擎将连续认证分数的初始分数设置为 λ，每当认证失败时，$\lambda=\lambda-1$。当 $\lambda<1$ 时，边缘服务器将断开和边缘设备的连接并终止边缘设备访问。据此得到第 i 个边缘设备的初始数字评分 DRS 为 I_j，即

$$I_j=\begin{cases}E+\varphi_{n+1}\lambda, & \lambda\geqslant 1\\ 0, & \lambda<1\end{cases} \tag{10}$$

信任引擎部署在第 i 个 ES 上。第 i 个 ES 对第 j 个 ED 进行身份认证，一旦 ED 的身份认证通过，ES 会为 ED 创建一个数字身份。在 ES 上部署的策略引擎会对 ED 数字身份进行信誉评分。本文同时考虑 ES 的信誉评分和 ES 的数字身份信誉评分，以得出边缘设备数字身份的推荐信誉评分 RED 为 G_{ij}。为了获得精确实时的 G_{ij}，DRSM 通过运用时间戳方案（例如设置间隔 $\Delta t=20$ s）告诉每个动作间隔上的各种优先级。在仿真系统中，直到现在的行动时间有 η 个间隔 $(t_1,t_2,\cdots,t_\eta)$。对第 k 个动作间隔，有 N_{tk} 个行动动作，G_{ij}^{tk} 的计算公式为

$$G_{ij}^{tk}=R_i^{tk}\cdot I_j^{tk} \tag{11}$$

G_{ij}^{tk} 可以用作边缘设备数字身份的初始信誉评分。如果边缘设备从未访问过系统，则初始信誉评分被设定为 0.5。

2.2.2　HRS 的计算

初始状态时，HRS 的值为 0。当经过身份验证的边缘设备第 2 次连接到边缘服务器时，根据 DRSM，领导边缘服务器上的信任引擎计算出该数字身份的 FRS 为 F，并作为初始 HRS，然后将其广播给其余所有的边缘服务器。当此边缘设备再次连接系统内任意边缘服务器时，领导边缘服务器上的信任引擎计算第 j 个 ED 第 p 次访问第 i 个 ES 时的 HRS 为 H_{ij}^{p}，即

$$H_{ij}^{p}=\begin{cases}\dfrac{\sum_{1}^{p-1}F_{ij}^{p-1}}{p-1}, & p>1\\ 0, & p\leqslant 1\end{cases} \tag{12}$$

2.2.3　*激励功能*

激励功能体现了对遵守策略引擎规定的边缘设备的激励措施。恶意的边缘设备进行访问时，有可能会破坏系统，因此它们的行为将会受到惩罚。定义激励函数 IRS 计算结果 S，公式为

$$S=1-\phi(\eta) \tag{13}$$

式中 $\phi(\eta)$ 表示边缘设备不遵守策略引擎规定的惩罚因子。至边缘设备和边缘服务器之间的当前动作时间（T）时，返回网络的边缘设备总数为 N_T，边缘设备违反规定的总数为 η_T。惩罚因子 $\phi(\eta)$ 的计算公式为

$$\phi(\eta)=y^{(N_T-\eta_T)/N_T}, 0<y<1 \tag{14}$$

当参数 y 减小时，$\phi(\eta)$ 增大；反之，当参数 y 增大时，$\phi(\eta)$ 减小。

策略引擎规定 RED、HRS 和 IRS 的权重分别为 α、β、δ，并将权重值发送给领导边缘服务器。最后，部署在领导边缘服务器上的信任引擎根据算法 1 计算 $\mathrm{DID}_{\mathrm{ED}}$ 的 F_{ij}。

$$F_{ij}=\begin{cases}\alpha G_{ij}^{tk}+\beta H_{ij}^{p}+\delta S, & \lambda\geqslant 1\\ 0, & \lambda<1\end{cases} \tag{15}$$

算法 1　计算最终信誉值

1. Input：行为 $N_{t_1},N_{t_2},\ldots,N_{t_\eta}$ 的时间 $t_1,t_1,\cdots,t_\eta$。

2. Output：最终信誉值 F_{ij}。

3. 至现在的行为时间时，ED 访问请求的总数为 N_T，ED 违反规则的总数为 η_T，ED 连接边缘服务器网络系统的总数为 p。

4. 进行基于 EigenTrust 的共识过程：

通过式（6）进行视图切换；

通过式（7）计算 R_i；

End。

5. 通过式（10）计算 I_j。

6. 通过式（11）计算 G_{ij}^{tk}。

7. 通过式（12）计算 H_{ij}^{p}。

8. 通过式（13）计算 S。

9. Return $\alpha G_{ij}^{tk}+\beta H_{ij}^{p}+\delta S$。

10. End。

3　实验与分析

3.1　实验环境及参数设置

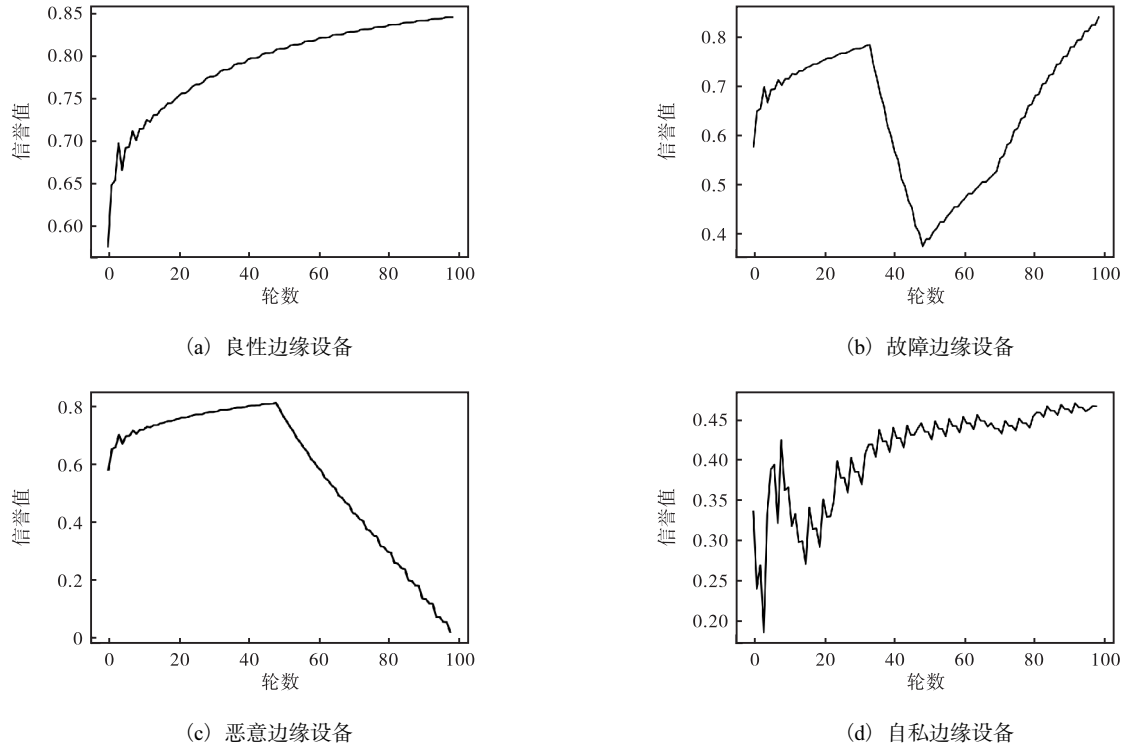
对 DRSM 进行仿真实验，在 Windows 11 中使用 Python 2.7.17 评估 DRSM 的性能。边缘设备被分为良性、故障、恶意和自私 4 种类型。良性边缘设备在系统的表现正常；故障边缘设备在系统中会出故障；恶意边缘设备一开始会表现得像良性边缘设备，后续会有恶意行动；自私边缘设备出于自己的目的，会表现得更加没有规律。

部署区域设置为 100 m × 100 m。零信任网络中分别随机部署良性、故障、恶意和自私边缘设备。模

拟的策略引擎设置良性边缘设备的 FRS 为[0.8, 1]，不确定行为边缘设备的 FRS 为[0.4, 0.8)，恶意边缘设备的 FRS 为[0, 0.4)。方程的参数设置为（N,m, n,α, β,δ,λ, y,Δt）=（30, 5, 7, 0.4, 0.3, 0.3, 8, 0.4, 20)。根据算法 1 计算每种边缘设备的 FRS。

3.2　信誉值更新

各种边缘设备的信誉更新过程如图 4 所示。在 Δt = 20 s 的情况下，横轴表示更新信誉评分的轮数，纵轴表示计算评分。



(a) 良性边缘设备　(b) 故障边缘设备

(c) 恶意边缘设备　(d) 自私边缘设备

图 4　各种边缘设备的信誉更新过程

Fig. 4　Reputation updated process of various EDs

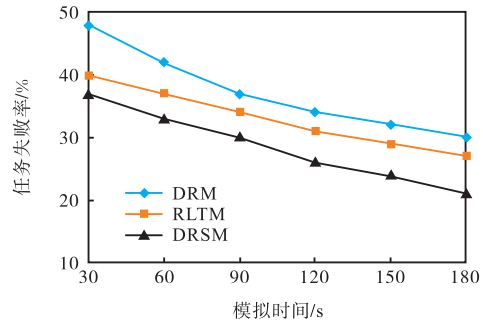
良性边缘设备的信誉评分在经历了小幅振荡后稳步上升。故障边缘设备一开始与正常设备具有相同的信誉值，并且还会经历平滑的增量；然而，出现故障后，信誉值会急剧下降。一旦有故障的边缘设备恢复，其信誉值就会再次开始上升。恶意边缘设备在加入系统时，信誉值会平稳增加；然而，恶意边缘设备一旦开始攻击，其信誉值就会明显恶化。值得注意的是，与故障边缘设备相比，恶意边缘设备的信誉值并没有显著下降，因为它仍然可以部分运行一段时间。自私边缘设备的初始行动是不确定的，这导致其信誉值波动；然而，在正常的访问尝试之后，自私边缘设备的行为逐渐转向不确定并表现出振荡增量。DRSM 可以区分边缘设备类型，这使策略引擎的决策更加安全可靠。此外，它还可以减少故障边缘设备、恶意边缘设备和自私边缘设备的负面影响，同时增强内生安全性。

3.3　与其他融合方法的比较

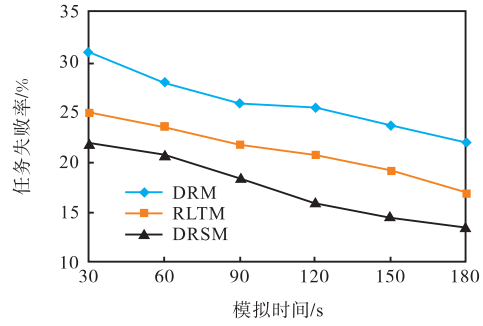
通过任务失败率[11]评估恶劣网络条件下信誉系统的可靠性，不同比例恶意边缘设备下任务失败率如图 5 所示。图 5 分别显示了网络中存在 35% 和 20% 恶意边缘设备时，3 种不同信誉模型（DRM[10]、RLTM[11]、DRSM）在 180 s 内任务失败率的变化。任务失败率得分越低，表明信誉机制的可靠性越高。

实验结果表明，在 35% 恶意边缘设备情况下，DRM、RLTM 和 DRSM 在开始时的失败率均超过 35%，这表明恶意边缘设备对任务执行的成功率影响较大。随着时间的推移，3 种模型都可以有效降低任务失败率，从而提高系统的可靠性。如图 5(a) 所示，DRSM 在所有时间段的任务失败率方面都较 DRM、RLTM 有一定的优势。DRSM 在实验模拟 180 s 后将任务失败率降低至 21%，并在实验后期降低 TRF 更加有效。如图 5(b) 所示，在 20% 恶意边缘设备情况下，表现出与 35% 恶意边缘设备情况下相似的趋势。DRSM 在 3 种信誉模型中均有最好的表现。在实验模拟 30 s 时，任务失败率为 22%；180 s 后任务失败率降至 12%，表现出了很高的安全性和鲁棒性。因

此，DRSM 在面对大量恶意攻击时更加稳健和高效。



（a）35%恶意边缘设备



（b）20%恶意边缘设备

图 5　不同比例恶意边缘设备下任务失败率

Fig. 5　Task failure percentage of different numbers of malicious EDs

4　结　语

本文提出一种基于零信任的数字信誉评分模型 DRSM。边缘设备的数字身份通过共识算法上传到区块链后，先由信任引擎评分，再由策略引擎对网络代理授权，以实现边缘计算环境下的零信任。仿真实验通过对不同类型设备访问的信誉值更新状况，以及在任务失败率方面的良好表现，验证了该方案的可行性和有效性。未来的研究将探索在确保安全前提下，优化零信任架构的性能。

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.

[2] 彭昇，赵建保，魏敏捷，等. 基于移动边缘计算的任务卸载优化[J]. 计算机系统应用，2023，32(4)：262–267.

[3] 郝敏，叶东东，余荣，等. 区块链赋能的 6G 零信任车联网可信接入方案[J]. 电子与信息学报，2022，44(9)：3004–3013.

[4] REN Y J，ZHU F J，QI J，et al. Identity management and access control based on blockchain under edge computing for the industrial internet of things[J]. Applied sciences，2019，9(10)：2058.

[5] LI S C，ZHANG N，LIN S Y，et al. Joint admission control and resource allocation in edge computing for internet of things[J]. IEEE Network，2018，32(1)：72–79.

[6] 于欣越，孙刚，张亚伟. 基于零信任的软件定义边界网络隐身技术研究[J]. 通信技术，2021，54(5)：1229–1234.

[7] SANDAL Y S，PUSANE A E，KURT G K，et al. Reputation based attacker identification policy for multi-access edge computing in internet of things[J]. IEEE Transactions on vehicular technology，2020，69(12)：15346–15356.

[8] DENG X H，LIU J，WANG L L，et al. A trust evaluation system based on reputation data in mobile edge computing network[J]. Peer-to-peer networking and applications，2020，13：1744–1755.

[9] LIAO Z F，CHENG S W. RVC：a reputation and voting based blockchain consensus mechanism for edge computing-enabled IoT systems[J]. Journal of network and computer applications，2023，209：103510.

[10] HUANG X M，YU R，KANG J W，et al. Distributed reputation management for secure and efficient vehicular edge computing and networks[J]. IEEE Access，2017，5：25408–25420.

[11] YUAN J，LI X Y. A reliable and lightweight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion[J]. IEEE Access，2018，6：23626–23638.

[12] LUKASEDER T，HALTER M，KARGL F. Context-based access control and trust scores in zero trust campus networks[J]. Sicherheit，2020，10(4)：53–66.

[13] GUO J，XU M. ZTESA：a zero-trust endogenous safety architecture：gain the endogenous safety benefit，avoid insider threats[C]//ISCAIS. Proceedings of International Symposium on Computer Applications and Information Systems. Shenzhen：ISCAIS，2022：192–202.

[14] MEHRAJ S，BANDAY M T. Establishing a zero trust strategy in cloud computing environment[C]//IEEE. Proceedings of 2020 International Conference on Computer Communication and Informatics. Coimbatore：IEEE，2020：1–6.

[15] LI D W，ZHANG E Z，LEI M，et al. Zero trust in edge computing environment：a blockchain based practical

scheme[J]. Mathematical biosciences and engineering, 2022, 19(4): 4196–4216.

[16] LIU D, YAN Z, DING W X, et al. A survey on secure data analytics in edge computing[J]. IEEE Internet of things journal, 2019, 6(3): 4946–4967.

[17] 埃文·吉尔曼, 道格·巴斯. 零信任网络: 在不可信网络中构建安全系统[M]. 奇安信身份安全实验室, 译. 北京: 人民邮电出版社, 2019.

[18] GAO S, YU T Y, ZHU J M, et al. T-PBFT: an EigenTrust-based practical Byzantine fault tolerance consensus algorithm[J]. China communications, 2019, 16(12): 111–123.

[19] KAMVAR S D, SCHLOSSER M T, GARCIA-MOLINA H. The EigenTrust algorithm for reputation management in p2p networks[C]//ACM. Proceedings of the 12th International Conference on World Wide Web. New York: ACM, 2003: 640–651.

责任编辑: 周建军

(上接第 36 页)

春果的形态和质构分析[J]. 乡村科技, 2022, 13(20): 75–79.

[18] VILLALOBOS M D, SERRADILLA M J, MARTÍN A, et al. Use of equilibrium modified atmosphere packaging for preservation of 'San Antonio' and 'Banane' breba crops[J]. Postharvest biology and technology, 2014, 98: 14–22.

[19] 曹建康, 姜微波, 赵玉梅. 果蔬生理生化实验指导[M]. 北京: 中国轻工业出版社, 2017.

[20] 刘耀娜, 王毅, 毕阳, 等. 采前乙酰水杨酸处理对厚皮甜瓜果实后熟及软化的影响[J]. 中国农业科学, 2017, 50(10): 1865–1875.

[21] HAGERMAN A E, AUSTIN P J. Continuous spectrophotometric assay for plant pectin methyl esterase[J]. Journal of agricultural & food chemistry, 1986, 34: 440–444.

[22] 高聪聪, 刘云飞, 董成虎, 等 新型保鲜剂处理对阳光玫瑰葡萄贮藏品质的影响[J]. 食品与发酵工业, 2020, 46(10): 147–151.

[23] 张广燕, 王莉, 杨建民, 等. 影响李果实贮藏保鲜的因素及贮藏技术[J]. 保鲜与加工, 2004(6): 11–13.

[24] 李春丽, 沈元月. 无花果果实发育过程中 ABA 和乙烯含量与果实成熟的关系[J]. 中国农业大学学报, 2016, 21(11): 51–56.

[25] OZKAYA O, ÇÖMLEKÇIOGLU S, DEMIRCIOGLU H. Assessment of the potential of 1-methylcyclopropene treatments to maintain fruit quality of the common fig (*Ficus carica* L.cv. 'Bursa Siyahi') during refrigerated storage[J]. Notulae botanicae horti agrobotanici cluj-napoca, 2014, 42(2): 516–522.

[26] SUN X K, YANG Q, GUO W D, et al. Modification of cell wall polysaccharide during ripening of Chinese bayberry fruit[J]. SCI Hortic-amsterdam, 2013, 160: 155–162.

[27] CUI Y Y, ZHAI Y L, HE J J, et al. AP2/ERF genes associated with superfast fig (*Ficus carica* L.) fruit ripening [J]. Frontiers in plant science, 2022, 13: 1040796.

[28] SENECHAL F, WATTIER C, RUSTERUCCI C, et al. Homogalacturonan-modifying enzymes: structure, expression, and roles in plants[J]. Journal of experimental botany, 2014, 65(18): 5125–5160.

[29] EUM H L, HAN S H, LEE E J. High-CO_2 treatment prolongs the postharvest shelf life of strawberry fruits by reducing decay and cell wall degradation[J]. Foods, 2021, 10(7): 1649.

[30] DENG Y, WU Y, LI Y F. Effects of high CO_2 and low O_2 atmospheres on the berry drop of 'Kyoho' grapes[J]. Food chemistry, 2007, 100(2): 768–773.

责任编辑: 郎婧