密级：公开　　中图分类号：TP393

☑全日制　□非全日制

浙江工商大學

硕士学位论文

（专业学位）

论文题目：面向物联网的零信任安全接入技术研究

作者姓名： 于镇栋

专业学位类别： 工程硕士

专业学位领域： 电子信息

研究方向： 物联网安全

指导教师： 蒋晓宁

提交日期：2023 年 6 月

Dissertation Submitted to Zhejiang Gongshang University for Master's Degree of Engineering

Zero Trust Secure Access Technology for the Internet of Things

Author: Zhendong Yu

Major: Electronic and Information Engineering

Supervisor: Xiaoning Jiang

Jun. 2023

School of Information and Electronic Engineering

Zhejiang Gongshang University

Hangzhou, 310018, P. R. China

摘要

近年来随着嵌入式软件、5G 网络、硬件设备等相关技术的快速发展，物联网设备产品以极快的速度升级换代，云计算服务也已经成为个人和企业广泛采用的信息服务模式。由于物联网设备的性能和物理空间有限，不能进行复杂计算和长期保留数据，因此诸多云计算服务供应企业（如阿里云、华为云等）提供了面向物联网设备和用户的服务，借此将需要算力的功能部署在高性能云服务器上，并将设备本地数据上传到云端，方便用户查看和管理。然而，由于云计算服务的网络需求更加多样化，传统的基于边界安全防护的访问控制策略不再适用于该场景。因此，本论文以物联网安全接入云计算服务为背景，结合当下流行的零信任网络架构和机器学习模型，提出一种创新的安全防护布局，旨在设计出适用于物联网设备和用户安全接入云计算服务场景的访问控制模型。论文的核心工作包括：

（1）提出基于 XGBoost 算法和 GRU 神经网络的攻击行为检测模型，针对物联网设备易受攻击和控制的缺点，使用机器学习算法检测访问主体攻击行为，用于后续信任值计算；

（2）提出基于访问主体行为的动态信任评估算法，该算法在模糊层次分析法的基础上，根据行为检测结果构建行为参数指标，并基于行为参数计算访问主体的信任值，同时引入奖惩机制、时间衰减因子、差异化权重等方法，使计算结果更准确；

（3）设计物联网零信任访问控制模型（BD-ZTBAC），该模型通过引入零信任思想，以访问主体行为参数作为信任计算依据。行为参数的获取和信任值的计算分别使用本文提出的行为检测模型和信任评估算法。使其能够克服传统访问控制模型灵活性差、准确性差、缺乏内部攻击防护、不适用于物联网场景等缺点，使访问控制决策更加可靠；

（4）模型整体评估，通过实验对信任评估算法和 BD-ZTBAC 模型进行验证和评估，并与其他算法和模型对比，证实本文提出的算法和模型在物联网领域实施的可行性和有效性。

关键词：物联网；云计算；零信任；机器学习；访问控制

Abstract

In recent years, with the rapid development of technologies such as embedded software, 5G networks, and hardware devices, IoT products have been upgraded at an extremely fast pace. Cloud computing services have also become widely adopted information service models for individuals and enterprises. Due to the limited performance and storage space of IoT devices, complex calculations and long-term data retention are not feasible. Therefore, numerous cloud computing service providers (such as Alibaba Cloud and Huawei Cloud) have offered services for IoT devices and users, deploying the functions that require computing power on high-performance cloud servers and uploading local data of device to the cloud for easy viewing and management. However, due to the increasingly diverse network demands of cloud computing services, traditional access control strategies based on boundary security are no longer applicable to this scenario. Therefore, this thesis proposes an innovative security protection layout based on the background of IoT secure access to cloud computing services, combined with the current popular zero trust network architecture and machine learning models. Aim to design an access control model suitable for the IoT device and user security access to cloud computing service. The core work of the thesis includes:

(1) Proposing an attack behavior detection model based on XGBoost algorithm and GRU neural network. In response to the vulnerability and control of IoT devices, machine learning algorithms are used to detect the attack behavior of the access subject for subsequent trust value calculation.

(2) Designing a dynamic trust evaluation algorithm based on access subject behavior. This algorithm calculates access subject trust values based on behavior detection results, based on fuzzy hierarchical analysis, and introduces reward and punishment mechanisms, time decay factors, differentiated weights, and other means to make the calculation results more accurate.

(3) Designing a zero-trust access control model for IoT (BD-ZTBAC). The model

introduces the concept of zero-trust, using access subject behavior parameters as the basis for trust calculation. The acquisition of behavior parameters and trust value calculation use the behavior detection model and trust evaluation algorithm proposed in this thesis This overcomes the shortcomings of traditional access control models, such as poor flexibility, accuracy, lack of internal attack protection, and unsuitability for IoT scenarios, making access control decisions more reliable.

(4) Overall evaluation of the model, verifying and evaluating the trust evaluation algorithm and BD-ZTBAC model through experiments, and comparing them with other algorithms and models, demonstrating the feasibility and effectiveness of the proposed algorithms and models in the IoT field.

Keywords: Internet of Things; Cloud Computing; Machine Learning; Access Control

目　录

表目录

图目录

1 绪论

本章将重点阐述物联网和云计算的发展背景、信任评估技术和零信任发展的研究现状，同时阐述本文主要研究内容和创新点，并简要说明论文行文结构。

1.1 研究背景和意义

1.1.1 课题研究背景

近年来，物联网、5G 通信技术、人工智能和云计算等技术快速发展，逐渐融入经济社会和人们日常生活中的各个领域中。根据中国信息通信研究院的调查研究结果显示，2021 年中国云计算市场规模已经达到 3229 亿元，较 2020 年增长 54.4%。在其中，公有云市场规模为 2181 亿元，增长幅度高达 70.8%。由此可以看出公有云市场正逐渐成为中国云计算市场增长的主要推动力量[1]。

越来越多的企业和个人选择将自己的服务部署在云环境中，通过云计算网络来提供高动态且易扩展的虚拟资源，包括一些物联网设备的拥有者也倾向于将设备收集到的数据上传到云端，以便于查看和分析。作为一种新的资源使用方式，云计算彻底改变了传统的网络服务模式，使得服务更触手可及，且服务的可扩展性和复用性也大大增强，但是伴随着这些优点的是更多安全隐患。由于云计算高度动态、使用分布式系统、非透明等特点，使得云环境中的安全问题日益严峻[2]。2017 年 9 月，美国个人信用评估公司 Equifax 披露了一个惊人的数据泄露事件，涉及到 1.43 亿美国居民的个人信息，占美国人口总数的 40%。因该次泄露事件的极高覆盖率使其成为美国历史上最严重的数据安全泄露事件；同年，AWS（亚马逊云科技）也发生了大规模的数据泄露，包括大量商业数据和 180 万选民的个人敏感信息。2016 年 10 月，Mirai 病毒[3]对全球物联网及其相关服务发动了一次大规模入侵，该网络病毒首先针对物联网智能终端设备进行攻击，随后利用这些智能终端设备作为跳板，进一步攻击数以万计的其他物联网设备和与其相关的网络服务，最后更是对部分云服务发动了 400GB 的分布式拒绝攻击（DDoS），最终导致大量物联网智能设备进入瘫痪状态，同时对部分云端服务造成了巨大的影响；2017 年 10 月，loTroop 网络病毒[4]攻击了高达两百多万台在线状态物联网设备，该病毒是一种危害极大的僵尸网络病毒，它的首要攻击对象是那些诸如摄像头、路由器等防护能力薄

弱的物联网智能设备，这些设备通常处于物联网边缘环境，安全性能有限并且存在大量安全漏洞。该病毒利用物联网设备的这些缺陷，造成了不可估量的损失。

由以上安全事件可以看出，云计算本身的安全问题在海量物联网设备接入的场景下被显著放大，如何确保物联网设备安全接入云计算服务成为一个迫切需要解决的问题。大量安全性能薄弱的物联网设备获得接入企业内网的权限，这些设备的接入模糊了网络防护的边界，因此云计算资源面临更大的安全挑战，传统的安全防护手段如防火墙、VPN等技术不再适用该场景[5]。并且这些安全威胁的根源中最为突出的问题就是网络信任问题，由于传统的网络设备的安全性能要优于物联网设备，这使得云计算网络资源能够对传统设备更加信任，但是物联网设备的特性导致云计算资源要对其提出更高的信任要求。大多数物联网设备厂商称安全漏洞是由于不断变化的网络威胁造成的，相同的物联网设备应用在不同的场景下会有不同的安全性能，因此传统基于身份认证的安全策略无法适用于该环境，如何守住物联网设备到云计算服务之间的这一关卡成为重中之重。

约翰·金德维格在 2010 年首次提出零信任架构（Zero Trust Architecture，ZTA），该架构可以用于保护企业或者个人一些对于安全性要求较高的资源。约翰·金德维格提出该架构的主要原因是他认为，企业系统应该在访问请求到达系统内部前验证其合法性，并且保证在验证成功前对所有请求“零信任”，这个规则将强制应用于系统内的所有资源，并且需要严格执行[5]。当一个访问请求发起时，ZTA 会首先判断其合法性，并在结束之后将其记录。评判请求合法性这一过程不会依靠单一标准，ZTA 会对每次请求访问的物联网设备及用户发起检测，借此对该次访问进行信任评估，以确定该资源是否可以被合法访问。如果被判断为不合法，此次请求将不能访问到任何资源[6]。零信任安全理念可以解决现有的物联网设备终端到云计算服务之间的安全问题。将身份认证和访问控制集中到计算力强大的云服务安全接入系统中，设备只需要提供部分自身的相关属性，通过安全接入系统分析和评估，就可以达到保护资源安全的目的。

1.1.2 课题意义

本文以实现物联网设备和用户安全接入云计算服务为目的，充分考虑云计算资源对安全的需求，针对传统物联网设备存在的风险，对物联网访问主体的行为进行检测和评估，然后参考 ZTA 架构中持续可信认证等理念，设计出适用于物联网场景的安全访问

控制模型，以保护云计算资源的安全访问。

本文尝试将零信任架构、机器学习以及用户设备动态信任评估三个概念合而为一，提出基于 XGBoost-GRU 行为检测机制的动态信任评估算法，并将信任评估算法结合到访问控制模型中，进而设计出能够有效阻挡物联网攻击并兼容用户和设备的物联网安全访问控制策略，实现物联网设备安全接入云计算服务，有效保护企业的云计算资源，对物联网安全领域的发展进行了补全和完善，拥有重大的实践意义。

1.2 国内外研究现状分析

本文主要研究方向包括物联网访问控制模型、基于信任的访问控制方法以及零信任架构，本小节将对这些领域的研究现状进行概述，并从中指出可以改进的点。

1.2.1 物联网访问控制模型研究现状

访问控制是一种通过对资源的访问、获取和操作进行身份认证和授权管理，使得被保护的资源能够在安全范围内被使用或受限使用的技术，是保护网络资源安全的重要手段[7]。访问控制模型根据使用者预先制定的策略对不同访问客体实施访问限制，其五大要素包括主体、客体、认证、授权以及策略。

与传统的访问控制模型相比，由于物联网和云计算环境的特点，两者之间的访问控制会面临更多的安全挑战：（1）访问主体、访问客体的种类十分多样化，网络边界模糊，数据传输过程中容易遭到信道攻击；（2）云计算资源拥有者无法提前预知资源会被何种访问主体以何种方式访问，并且由于云服务常用分布式结构，更无法预知资源会在何处被访问；（3）物联网终端设备安全性能较弱，容易受到攻击，所以访问可信度降低，难以直接信任；（4）同时会有设备和用户共同访问云服务，协议和访问形式多样化，难以通过单一方法保证安全性。为了应对以上安全隐患，Ouaddah 等人总结物联网访问控制应该遵循以下 8 个原则[9]：

（1） 协同性：访问控制系统允许各个主体制定适合自己的访问控制策略，并且能够和其他主体的策略互通兼容；

（2） 自适应策略：访问控制策略能够根据上下文进行自适应动态调整，实现动态控制；

（3） 细粒度：物联网设备种类多样且在不同场景下会对云服务进行不同类别的访问，所以访问控制也需要考虑这些细分的情况，能够提供粒度更小的访问控制功能；

（4） 分布式自治系统：每个实体都可以制定自己的访问控制策略，以满足物联网环境中分布式安装的智能设备的访问控制需求；

（5） 异构性：由于物联网设备差异大，所使用的协议也不尽相同，所以在进行访问控制时要根据设备的区别做出不同的访问控制策略；

（6） 轻量性：物联网设备性能往往不足以支撑复杂的访问控制系统，所以对于物联网设备的负担要尽可能小，高性能的云端控制服务可以承担主要的访问控制功能；

（7） 可扩展性：访问控制系统需要做到可扩展、易扩展，可以适应越来越多的物联网设备、应用以及用户；

（8） 易用性：访问控制功能应该易于管理和修改，方便缺少相关技术知识的运营维护人员使用该系统。

不同云计算访问控制技术的对比结果如表 1.1 所示。

表 1.1 不同的云计算访问控制技术的对比

方法/模型	机制	技术	优点	缺陷	适用场景
RBAC	拓展的传统方案	RBAC	动态性	拓展性差	自适应访问控制
ABAC[10]	拓展的传统方案	ABAC	细粒度	效率低	大规模信息系统
CTAC[11]	多租户技术	共享机制	有效性	复杂性高	资源共享频繁
文献[12]	多租户技术	敏感度	安全性	拓展性差	虚拟资源分配
UCON	拓展的传统方案	UCON	易拓展	授权管理复杂	分布式跨域环境

表中列举了各种云访问控制技术的优点、缺点以及适用场景。通过该表可以看出，虽然云访问控制技术在近年来不断发展，但是仍然存在一些可以改进的方面，例如：（1）在细粒度要求方面，大部分访问控制技术难以支持；（2）大部分访问控制技术拓展性较差，且对于时间、位置等因素比较不敏感；（3）部分访问控制技术机制较为陈旧，难以抵御来自系统内部的攻击，不适用于物联网接入云计算服务的复杂环境[13]。

1.2.2 基于信任的访问控制研究现状

文献[7]中指出，目前物联网领域访问控制模型的发展方向主要是将互联网中成熟的基于属性的访问控制（Attribute Based Access Control，ABAC）、基于角色的访问控制（Role Based Access Control，RBAC）、UCON（Usage Control）等访问控制模型经过适当修改后移植到物联网环境中。这些传统模型经过数十年的发展，已具有较高的可靠性和实用性，因此只需要针对物联网应用环境的特点进行轻量修改和定制就可以满足使用的要求。但是这些传统的访问控制模型并不能适用于当今愈加复杂的网络环境，并且大部分模型无法抵御来自系统内部的攻击，从而带来巨大安全隐患。

因此中国工程院院士沈昌祥于 2017 年提出“用可信计算构筑云计算安全”的口号，并指出国内云计算发展初期只注重“计算”，忽略了安全方面的问题，云计算资源也需要有自己的“免疫系统”，而信任评估可以推动建立可信、可控、可管的网络环境[14]。通过可信计算技术，可以实现云计算的可信度评估、数据隐私保护、应用程序保护等功能，从而提高云计算的安全性。这些措施可以有效地防止黑客攻击、数据泄露和恶意软件等威胁，保障云计算资源的安全和稳定运行。

对于传统 ABAC 模型，关于该模型的研究方向主要在以下几个方面：（1）授权方式[15]：主要探讨如何根据访问主体属性进行授权；（2）策略冲突[16]：研究策略之间冲突的情况和解决方案；（3）策略迁移[17]：研究不同域之间策略迁移的手段和方式。然而这类研究并不能解决来自内部的威胁，例如，当获得权限的访问主体被入侵，系统无法察觉其恶意行为的存在，攻击者可以盗用已经获得访问权限的物联网设备和用户的身份进行入侵攻击。但是如果将信任因素与 ABAC 模型结合，就能起到动态访问控制的效果，因为信任评估的结果是根据访问主体行为计算出的一个动态值，是可以根据不同情况修改的，这样就能够解决传统 ABAC 模型的局限性，防御来自系统内部的攻击[18]。

文献[19]在 RBAC 模型的基础上，引入了信任约束和用户属性等模型元素，提出了 TA-RBAC 访问控制模型。该模型取消了单一的用户角色分配方式，而是以信任值作为角色分配的决定性属性，只有当用户的信任值达到访问控制策略要求的信任阈值时，才能获得该阈值所对应的角色，同时能够得到该角色对应的访问权限。而且这个分配角色是一个动态的过程，该模型会根据用户的属性动态调整用户信任值，以达到动态分配控

制权限的目的。文献[20]基于传统 ABAC 模型，引入动态用户信任度属性，并且针对云计算环境分布式、多域等特点，考虑了不同安全域之间的时间有效性、评价相似性、惩罚机制等多种因素，提出了 CT-ABAC 访问控制模型。该模型会使用多种用户属性来衡量用户的可信程度，其中包含信任值这一属性，同时实现了动态判断信任度功能，能够有效改善恶意用户访问的现象。文献[21]在 T-ABAC 访问控制模型的基础上，引入了主体信任度属性相似性度量。通过计算某个租户与绝对安全租户之间信任度的相似度，来判断该租户是否也是安全租户，当相似度达到策略的阈值，可以将该租户看作与绝对安全租户对等可信。该属性可以减少对主体信任度的复杂计算，仅对比两个不同租户属性的相似度就可以达到访问控制的目的，显著提高了访问控制策略执行的速度。文献[22]基于 UCON 模型和零信任思想，分析访问主体的特点，根据分析结果对访问主体的行为制定信任评估标准，并且能够对访问主体进行持续信任评估，在此之外更是结合了异常情况监控，降低访问主体的恶意行为对系统的影响，提高模型安全性能。

综上所述，国内外学者对于信任评估访问控制模型已经获得了许多研究成果，然而对于信任值的具体计算方法并未达成共识。此外大部分访问控制模型只是在理论阶段，没有进行系统化验证。并且一些学者所研究的访问控制模型本身也存在不少缺陷，所以在物联网场景下将信任评估机制与访问控制技术相结合是未来发展趋势，这种方法不仅可以解决传统模型细粒度不足、动态性差等问题，还可以适应物联网的复杂环境。

1.2.3 零信任架构研究现状

零信任架构自 2010 年由 John Kindervag（约翰·金德维格）提出以来，已经得到了社会广泛的认可[23]。云计算、大数据和移动互联网的飞速发展是零信任架构得到普及的最大推动力。随着云计算和大数据逐渐成为当今互联网必不可缺的一部分，带来了更多安全方面的挑战，这个挑战不仅来自于外部的攻击，内部威胁的数量也愈来愈多。尤其是在物联网环境下，攻击者可以通过存在漏洞的物联网终端设备轻易入侵到云计算网络中，已经接入网络中的设备和用户也变得不可信。面对此类威胁，零信任架构可谓是一剂良药。零信任架构的安全理念为“默认不信任网络内外的任何用户、设备”，这一理念不仅可以防御外部攻击，也可以应对内部威胁。每次有设备或者用户访问云计算资源，都要单独加以验证该访问的合法性，并会根据上下文进行动态评估。

零信任发展至今，衍生出三种主流技术方案分别是：软件定义边界（SDP）、身份和访问管理（IAM）和基于身份微隔离（MSG）[24]。不同方案适用于不同场景，能够针对不同层面的问题。其中 SDP 的重点是根据软件服务需求定义访问边界，仅允许合法的客户端访问请求通过成功访问服务端[25]。

在国外，许多科技巨头已经开始将零信任架构整合到企业网络中。Google 于 2017 年就完成了 BeyondCorp 计划，该计划舍弃了传统的 VPN 技术，转而采用零信任架构，该架构要求用户不论在内外网都需要进行身份认证和访问控制。此后其他一些国外科技公司也相继推出适合自己的零信任方案，如 Duo、OKTA、PingIdentity 等。随着各大公司扩大投入和研究，零信任架构的发展速度非常快，Gartner Group 公司更是推测，到 2023 年会有超过 60%的企业舍弃传统 VPN 技术，取而代之的是基于零信任架构的安全防护手段[26]。美国国防创新委员会从 2019 年起陆续提出零信任指导建议，不断推动零信任架构在国防产业中落地，通过零信任架构的普及来提高网络空间话语权[27]。

零信任不仅在国外发展势头迅猛，国内各大网络安全和物联网厂商也在零信任架构上加大投入。2016 年腾讯、360、完美世界等厂商开始在公司内部实施零信任改造。在 2020 年初疫情暴发时期，腾讯已经实现每日 10 万台设备接入的全员远程办公。随后奇安信、阿里、华为、深信服、启明等厂商也成功设计出零信任解决方案。2022 年底，中国信通院发布零信任发展洞察报告，报告中显示，国内零信任赛道竞争激烈，各大企业都在不同领域寻求创新和突破，足以证明零信任在国内发展势头十分迅猛，并且可以解决企业在网络安全方面的问题。国内各企业零信任产品的相关信息如表 1.2 所示。

表 1.2 国内企业零信任产品概况

企业	产品名称	身份安全	网络安全	应用安全	数据安全	终端安全	安全管理
腾讯云	腾讯 iOA 零信任安全管理系统	√	√	√	√	√	√
天融信	天融信零信任 SDP 控制系统	√	√		√	√	√
奇安信	奇安信零信任安全解决方案	√	√	√	√	√	√
绿盟科技	绿盟科技零信任安全解决方案	√	√		√	√	√
深信服	零信任安全办公解决方案	√	√	√	√	√	√
安恒信息	零信任数字化安全接入平台	√	√			√	√
浪潮	浪潮云御零信任控制系统	√	√	√			√
阿里云	办公安全平台 SASE	√	√	√	√		√

通过分析表中的数据可以得出，零信任是当下物联网接入云计算服务安全问题的优秀解决方案。其理论和实践成果足以推进物联网安全方向的发展，为基于零信任的物联网安全访问控制系统的设计与构建提供了充足的条件。

1.3 主要研究内容和创新点

本文针对当今物联网和云计算面临的安全问题以及该领域访问控制模型的缺陷，将零信任架构与基于属性的访问控制模型相结合，提出一种结合行为检测机制的零信任访问控制模型（Behavior Detection-Zero Trust Based Access Control，BD-ZTBAC），在信任评估阶段结合 XGBoost-GRU 行为检测模型，使用机器学习技术辅助用户和设备信任值的计算，使得访问控制更加高效和可靠。以下是本文具体研究内容和创新点：

（1）物联网环境复杂，设备种类繁多，协议多样，且物联网终端设备安全性能较差，容易遭受入侵和操控，这使得云计算资源易受到内部威胁。为了抵御内部威胁，需要通过访问主体行为判断其可信度，本文为了使信任评估所需的行为参数更可靠而引入基于 XGBoost 模型和 GRU 神经网络的行为检测机制，用以识别攻击行为，为后续信任值计算提供更可靠的依据；

（2）提出基于行为检测结果的动态信任评估算法，该算法在层次分析法的基础上进行优化，根据行为参数的重要性设置不同权重，综合所有行为参数计算访问主体信任值，同时使用奖惩机制、时间衰减因子、差异化权重等手段提高计算结果的准确度；

（3）对云计算环境中主流的访问控制技术进行研究，结合物联网场景下主要面对的安全问题，总结出传统访问控制技术需要改进的点，提出结合物联网行为检测的零信任访问控制模型（BD-ZTBAC），该模型通过基于行为的信任评估算法实现对访问主体的持续验证，根据访问主体信任值和云计算服务信任阈值实现比传统模型更细粒度的访问控制，与此同时能够迅速发现恶意访问主体，拦截其访问行为；

（4）基于 BD-ZTBAC 模型实现仿真测试系统，通过构造不同行为的用户和设备，对系统进行访问或攻击，验证模型能够有效防护物联网安全攻击。

1.4 论文组织结构

本文正文部分共分为六章，每个章节内容概括如下：

第一章 绪论。综合分析本课题的研究背景和课题意义，对国内外访问控制技术和物联网系统安全技术的发展现状做了简单阐述，指出该领域现存的问题，并概述本文主要研究内容和创新点。

第二章 相关技术概述。该章节对本课题所涉及的核心理论和方法进行概述，主要包括云计算服务、访问控制、零信任架构、与行为检测技术四个方面。

第三章 基于 XGBoost 和 GRU 的智能行为检测模型。本章首先概述该模型所使用的算法和模型结构，然后选取合适的物联网流量数据集，使用 XGBoost 算法对数据进行特征选取，特征降维后使用 GRU 神经网络模型训练，并将结果与其他机器学习模型对比，证实模型的高准确度。

第四章 基于访问主体行为的动态信任评估算法设计。本章提出一种根据访问主体行为参数计算信任值的动态信任评估算法。该算法在模糊层次分析法的基础上进行优化，通过引入奖惩机制、时间衰减因子和差异化权重等手段，提高计算准确度，并且能够将访问主体的行为快速体现在信任值变化上，提升算法灵敏度。

第五章 物联网可信接入访问控制模型设计与仿真实验。本章首先提出结合行为检测的零信任访问控制模型（BD-ZTBAC），该模型在行为参数采集方面使用第三章提出的行为检测模型，提高参数的可信度；信任值计算方面使用第四章提出的信任评估算法，保证计算结果的准确度和灵敏性。然后根据零信任架构和控制模型实现安全接入系统，并通过仿真实验验证信任算法的性能和访问控制模型的控制效果，最后对结果进行整体分析。

第六章 总结与展望。对本文研究做出总结，提出未来改进方向和展望。

2 相关技术概述

2.1 云计算服务概述

2.1.1 云计算基本概念

云计算是一种凭借网络“云”技术将数据计算处理过程交由云上分布式服务程序处理的服务模式。云服务器接收到用户请求后，使用分布式服务器组成的系统对用户提交的请求进行处理和分析，再将计算得到的结果返回给用户。用户可以不用在本地部署程序，依据自身的需求向云计算服务供应商支付费用，而这些费用会根据用户的请求类型调整。用户可以通过对应的云计算服务获取诸如服务器资源、文件备份、数据存储及处理等资源和服务。

根据云计算提供资源和服务的区别，通常可以将其分为以下 3 类：将基础设施作为服务（Infrastructure-as-a-Service，IaaS）、将平台作为服务（Platform-as-a-Service，PaaS）、将软件作为服务（Software-as-a-Service，SaaS）。其中本文聚焦 SaaS 类云计算服务，该种云计算服务针对性强，它将某些特定的应用软件功能封装成云服务，供用户或设备调用[28]。

除了基于资源和服务区别的三种分类，云计算还有四种部署模型[29][30]：

（1）私有云：云计算的基础设施是私有的，在企业或者组织内部的访问主体拥有访问权限。私有云平台不属于共享资源，对于数据隐私要求高的情况下是首选部署模型，但是建设和维护成本高；

（2）社区云：云计算服务可由社区内的组织享有，非社区内部的组织无权访问服务，社区云由社区内所有组织共同运营和管理；

（3）公有云：云计算服务向公众提供，服务会部署在开放的网络环境中，为访问主体按照需求提供服务。公有云的经济成本较低，也是现有云计算服务的主要部署方式，但是由于网络环境的公开性，其安全性是最低的，所以安全策略是公有云部署模型中至关重要的组成部分；

（4）混合云：云基础设施有以上三种部署方式混合组成，云计算服务供应商一般会提供私有云和公有云组合的模式。该模式可以获得多种部署模型的优势，但是由于模型

复杂度提高，维护和建设成本也会增加，并且需要对服务和数据的安全等级进行划分并部署在不同的模型中。

为了适应当今网络的快速发展，云计算很好地解决了用户在软件开发、服务部署时的难点。云计算有以下优点：1）敏捷性：云计算可以使用户快捷且轻松的使用各种技术，而不用额外开发。对于一些共通的计算服务，通过使用位于云服务器上的服务，可以减少单独开发的成本，且不用额外花费时间搭建本地服务，从而可以更快进行创新；2）扩展性：用户可以根据业务场景需求合理预置资源，不用为了高峰情况而过度预置资源，通过云计算优异的可扩展性灵活应对不同的业务场景；3）节省成本：云计算将固定资本支出转为可变支出，并且云计算服务的费用通常按照实际用量付费，可以减少不必要的浪费；4）快速部署：位于云服务器上的云计算服务由于可以在任何地区访问，能够提高部署服务的速度[31]。

2.1.2 云计算安全问题

虽然云计算拥有很多优点，但同时也因为其特点面临很多安全威胁[32]，具体安全威胁如表 2.1 所示。

表 2.1 云计算面临安全威胁

威胁层次	威胁类型	示例
IaaS	外部威胁	SQL 注入、DDoS、平台渗透
	内部威胁	虚假服务、资源窃取、共存攻击
PaaS	破坏机密性	管理者窃取数据、侧信道攻击
	破坏可用性	DoS 攻击、资源抢占攻击
SaaS	破坏机密性	管理者窃取用户隐私
	破坏可用性	恶意的 SaaS 提供商破坏用户终端，提供虚假业务

来自系统外部的入侵者通常会凭借系统或者平台的漏洞、网络防护不足等缺陷发起攻击，这部分攻击并不是云计算特有的，所有的计算机系统和服务都面临外部威胁。而内部威胁是随着云计算环境的普及而带来的特殊威胁，并成为了影响云计算服务安全的主要原因。对于内部威胁，不能单一凭借密钥、属性等因素判断，需要结合用户和设备的行为来评估访问是否合法，并且需要一个动态的评估机制，不能使用静态方法判断用

户的可信度[33]。

2.1.3 云计算与物联网

近几年随着物联网的快速发展，在物联网设备的运行过程中会产生大量的数据信息，而这些数据信息也是属于企业无形的财产。通过对这些数据进行计算和分析，可以给企业带来巨大的收益，因此许多企业创建云端、云技术平台用于处理这类数据。但是由于物联网设备一般不具备强的计算性能，而且企业需要将物联网设备数据集中分析，所以云计算服务在物联网中也扮演了重要的角色。物联网设备通过调用位于云服务器上的服务接口，将自身收集到的数据上传，或者将自身无能力计算的复杂功能委托给云计算服务完成。总而言之，物联网的发展和广泛应用需要云计算提供基础保障。而近几年大数据和云计算技术的广泛应用也是物联网快速发展的重要原因之一[34]。

云计算和物联网结合可以解决物联网的以下缺陷：（1）不稳定性：云计算可以弥补物联网中服务器节点的不稳定性，可以减少由于物联网设备运行异常带来的不良后果，并且相比物联网设备来说计算更加可控[35]；（2）计算资源利用不当：庞大的数据量可能会对性能不足的物联网设备产生影响，严重时可能会产生程序崩溃、超出存储容量等致命问题；（3）资源共享困难：由于不同物联网设备所处的环境差异很大，其数据很难在设备与设备之间共享，所以可以通过云计算实现资源的共享和流通，物联网设备将数据存储在云计算服务器中，其他设备可以使用对应服务获取此类数据。

但是云计算和物联网结合可能会导致更多安全问题，除了物联网本身的安全问题，还需要考虑云计算环境的威胁，所以需要一个更加完善的访问控制模型来保证系统的安全。

2.2 访问控制相关技术概述

访问控制技术是保证物联网设备和用户安全接入云计算环境的重要屏障。下面首先对访问控制技术进行简要概述，并根据云计算系统安全的需求制定访问控制模型的性能评价指标。

2.2.1 物联网访问控制技术

访问控制技术一般由三个要素组成，包括主体、客体和访问控制策略[36]。主体通常是指访问请求方，在物联网中一般指代物联网设备和用户；客体一般是指被访问的资源和服务，如接口、数据、文件等；访问控制策略通常是由一系列规则组成，它们被用来判断访问行为的合法性。最基本的访问控制模型如图 2.1 所示。

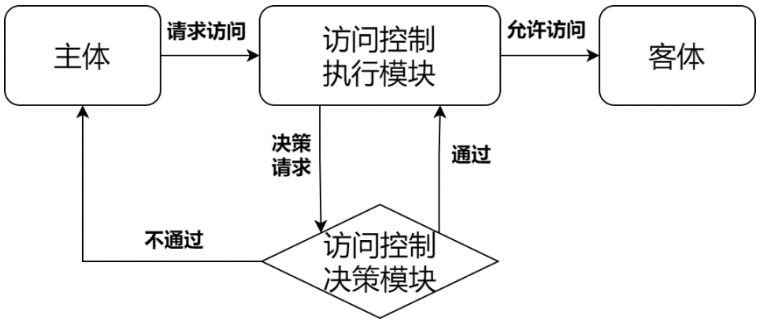

图 2.1 基本访问控制模型

访问控制方案可以根据实现方式划分为访问控制策略、访问控制模型和属性加密机制。整理内容如表 2.2 所示。本文研究主要聚焦于访问控制模型这一方面。

表 2.2 云计算访问控制技术

名称	常用方法	作用
访问控制策略	访问控制表、访问控制矩阵	准入控制
访问控制模型	DAC，TBAC，RBAC，ABAC，UCON	权限分配
属性加密机制	KP-ABE，CP-ABE	数据加密

2.2.2 访问控制模型性能评价体系

访问控制模型种类繁多，不同模型应用在相同环境中会有不同性能表现，为了评价本文设计的访问控制模型性能的好坏，需要引入物联网安全接入云计算访问控制模型性能评价体系。该体系中的性能评价指标是评价研究成果的标准，通过不同的指标反映模型的运行效率、运行性能、安全性等不同层面的表现。本课题将从这些指标分析最终研究结果，具体指标及说明如表 2.3 所示[37]。

表 2.3 物联网环境下云计算访问控制模型性能评价指标

参数	说明
安全性	模型的可证安全性能如何
细粒度	模型能否实现细粒度访问控制
主客体属性	模型是否支持通过主客体属性来进行访问控制
时间属性	时间属性能否影响访问控制结果
物联网环境	模型是否适用于物联网环境
云计算环境	模型是否适用于云计算环境
授权灵活性	模型能否灵活对主体授权
授权因素	影响主体授权的因素有哪些，因素的选择是否科学
可扩展性	模型能否简易扩展规模
异构性	模型能否应对不同物联网设备的请求

2.3 零信任架构（ZTA）概述

零信任架构（ZTA）打破传统网络安全模型单纯依靠身份认证建立信任的旧式思维，并指出身份认证只是信任的先决条件之一，在进行身份认证后还需要对访问主体进行信任评估。只有在信任值达到一定阈值时，访问主体才能被认为是“可信”的，这样能够极大增加决策的可靠性。下面将从信任的概念及分类、信任评价参数和零信任架构组成部分三方面简述零信任相关技术。

2.3.1 信任的概念和分类

“信任”这一概念最初来源于社会科学，是一种难以度量的主观心理认知。不同学科领域对于“信任”的定义不尽相同[38]，其中对于网络系统中的“信任”形式化问题最早于 1994 年由 Marsh 博士提出，为信任相关理论在计算机领域中的发展和应用做出了卓越的贡献[39]。随后 Blaze 在 1996 年提出了“信任管理”的概念[40]，并尝试使用信任管理机制来解决分布式系统的安全问题。随着分布式系统和开放式应用系统技术的迅速发展，系统不断提升的开放性和复杂性也带来了诸多安全问题，对于安全性的要求也越

来越高。与此同时，由于 5G 时代的到来、物联网设备海量接入云计算服务，云计算服务系统的开放性和复杂性到达前所未有的高度，这导致物联网场景下传统的静态访问控制策略难以满足安全需求。Mirai 僵尸网络袭击等针对物联网的大规模袭击也印证了这一点，这促使物联网领域研究人员将目光转向基于信任的访问控制技术，通过评估物联网访问主体的信任值，然后根据信任值与访问客体信任阈值的对比结果进行授权，尽量降低主观因素影响，提高网络系统的安全性。

目前为止，计算机研究领域对于“信任”并没有一个明确的统一定义，不同细分领域的研究人员对于信任的理解也存在较大差异[41]。大部分研究人员认为信任本身可以携带丰富的属性，也就是说可以通过种类丰富的数据来评估信任值。通常信任可以分为以下几种类别，具体类别和释义如表 2.4 所示。

表 2.4 信任的分类

类别	释义
身份信任	通过静态方式验证实体身份的可信程度
行为信任	通过实时监控、行为检测和日志分析等方式，对访问主体的各种访问行为进行信任评估，并且能够动态地调节该访问主体的权限
直接信任	在直接连接关系的实体之间产生对彼此的信任
间接信任	不同系统的节点之间通过各自系统的信任值建立信任关系
域间信任	以域为单位，通过非本域的信任评估算法评估域内某节点的可信程度
域内信任	以域为单位，通过域内的信任评估算法评估域内某节点的可信程度
局部信任	源节点和目标节点通过信任网络计算两者之间的信任度
全局信任	目标节点在整个信任网络上的整体信任度
一元信任	仅通过信任程度一个元素来判断节点的可信程度
多元信任	用信任、不信任和不确定等多个元素判断节点的可信程度

2.3.2 信任评估算法评价参数

与访问控制模型相同，信任评估模型的好坏也需要科学的评价参数，用以验证算法

的优劣。现有的一些应用在物联网领域的信任评估算法采用例如 FANP（uzzy Analytic Network Process）、FAHP（Fuzzy Analytic Hierachy Process）、AHP（Analytic Hierachy Process）、贝叶斯理论、机器学习等方式评估用户信任度。基于对这些算法模型的过程和结果的对比，结合物联网环境特点，总结出以下七个信任评价参数，如表 2.5 所示[42]。

表 2.5 信任模型评价参数

参数	说明
灵活性	信任机制动态调整和持续更新信任值的能力
时间衰减性	不同时间间隔的同一行为是否存在信任衰减
抗攻击性	检测并抵御攻击行为的能力
奖惩机制	根据节点的行为，对其进行激励和惩罚
敏感性	感知访问主体行为变化并及时应对的能力
可扩展性	模型扩展的难易程度
量化方法	量化信任值所用方法的复杂度和实施难易度

本文将根据上述评价参数对传统信任评估算法做出优化，设计出能够满足这些性能的动态信任评估算法。

2.3.3 零信任架构组成部分

零信任理论需要以下五个前提作为支撑：（1）网络时刻处于危险的环境中，所有的设备和用户默认为不可信；（2）网络威胁可以来自外部，也可以来自于内部；（3）网络的位置（IP 地址）并不足以决定访问请求是否安全；（4）所有设备、用户和流量都应当经过认证和授权，且单一身份认证并不足以确认其安全性；（5）安全策略必须是动态的，需要考虑上下文，且影响信任评估结果的因素要尽可能多[43]。

在美国国家标准技术研究所发布的《零信任架构》草案给出了零信任的访问控制模型如图 2.2 所示[44]。

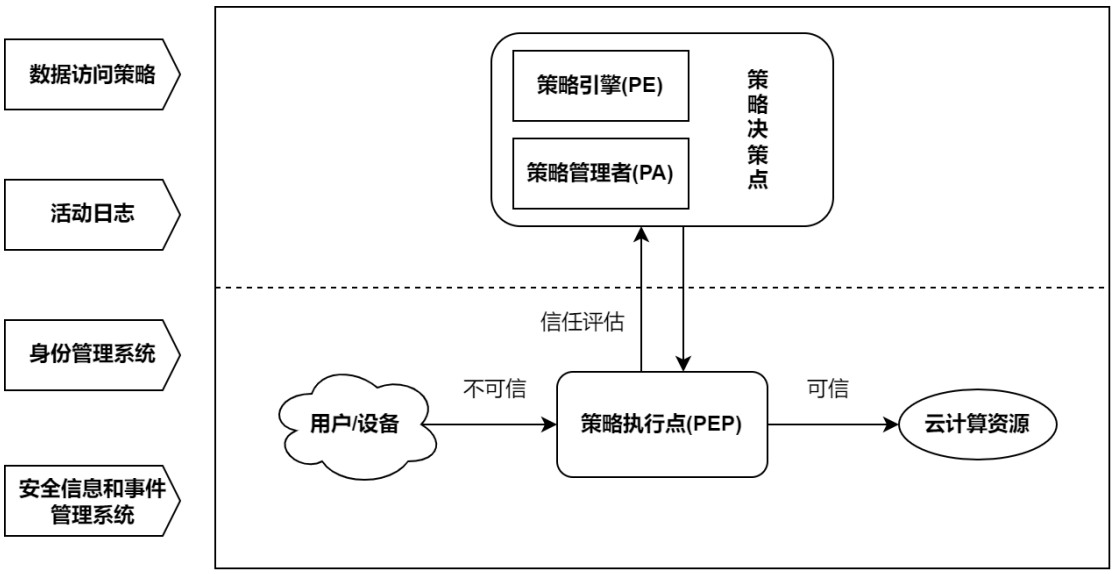

图 2.2 零信任访问控制架构图

下面将根据该模型结构图简述零信任架构的组成部分：

（1）策略引擎（Policy Engine，PE）：该组件会根据核心信任算法（Trust Algorithm，TA），判断访问主体的访问请求是否合法。PE 利用设备和用户的信任因素作为 TA 的输入，再依据 TA 输出的信任值和对应云计算资源的访问策略，决定是否信任该次访问。本文将在第四章详细描述信任评估算法；

（2）策略管理者（Policy Administrator，PA）：该组件与 PE 关联性极强，依赖于 PE 计算的信任值来决定该次访问的最终放行结果；

（3）策略执行点（Policy Enforcement Point，PEP）：该组件负责根据 PA 的决策来建立或关闭主客体之间通信连接。并且始终监视这次连接，保证通信的安全性；

（4）功能插件：这类组件是指能够提供评价信任值所需数据的插件，包括并不仅限身份管理系统组件、活动日志组件、行为检测组件等[47]。这些组件会提供行为参数、历史行为日志等用于评判信任值的信息，作为策略引擎的参考依据。由于这些信息能够间接影响信任值的计算结果，因此选择高性能的功能插件非常重要。

2.4 物联网行为检测技术概述

零信任架构要求安全策略是动态的，需要持续性地对信任进行评估。而在物联网环境下，由于物联网终端设备较弱的安全性，针对物联网设备的网络攻击十分常见，物联网终端设备会受到攻击从而带来内部安全威胁。为了使得访问控制模型能够更好适应物

联网环境，行为检测技术是必要的，该技术可以给信任评估算法提供访问主体相关行为参数用于信任值的计算，提高访问控制模型的安全性。

关于物联网用户和设备的行为可以分为以下四种：

（1）攻击行为：指访问主体对系统进行的攻击，该类行为包括外部入侵行为和内部异常操作[48]，如越权访问、端口扫描、DoS 攻击等，该类行为对于系统的危害性最大，需要使用高效的手段进行识别检测；

（2）访问行为：指访问主体在对客体进行访问时的各类行为统计，如访问成功率、访问请求频率等；

（3）网络行为：指访问主体本身网络的变化行为，如流量变化、IP 复杂度、平均请求时延等。该类行为能够描述访问主体网络环境的改变情况，一般较为稳定的网络行为能表示该访问主体具有较高的可信度；

（4）硬件行为：指访问主体硬件自带属性的变化行为，如 MAC 地址、地理地址等。对于物联网设备来说硬件属性几乎不会发生变化，所以可以将硬件行为作为安全性的评估因素。

本文算法将通过这四类访问主体行为，计算其信任值。

2.5 本章小结

本章主要简述了云计算的基本概念及其在物联网领域的应用，访问控制模型以及模型评判标准，并引入零信任网络和信任相关概念，最后说明零信任架构中必不可少的行为检测技术。从下一章开始将深入探讨物联网环境下的安全接入技术。

3 基于 XGBoost 和 GRU 的智能行为检测模型

本章根据前文概述的物联网环境特点和零信任框架的模型，进一步研究如何解决物联网设备和用户接入云计算服务场景下的安全问题，提出 XGBoost-GRU 智能行为检测模型。该模型使用 XGBoost 算法进行特征选取，使用 GRU 神经网络对时间序列数据进行攻击行为检测，借此区分不同种类的攻击行为，并输出检测结果用于信任评估算法对访问主体进行信任值的计算，能够满足零信任框架持续验证的需求。

3.1 XGBoost 算法概述

XGBoost（eXtreme Gradient Boosting）极端梯度提升算法，是一种基于决策树和梯度提升算法的改进型集成算法[46]。该算法有优秀的学习效果和训练速度，近几年被广泛应用于分类任务，在机器学习领域和数据挖掘领域的相关建模比赛中都有良好的表现[47]。该算法的原理是通过迭代地构建多个弱分类器来对数据样本的特征进行评估和挑选，并将这些弱分类器的输出结果汇总，从而将模型整体训练成强分类器，以实现更准确的分类效果。XGBoost 中可以选择分类回归树和线性分类器作为弱学习器。

研究 XGBoost 的原理先从 XGBoost 模型中的单棵决策树出发，假设 x 和 y 是模型的输入特征和输出结果，其中 y 是连续变量，则给定的训练集可以表示为：

$$D = \{(x_1, y_1), (x_2, y_2), \cdots, (x_N, y_N)\} \tag{3-1}$$

其中$x_i = \{x_{i1}, x_{i2}, \cdots, x_{im},\}, x_{ij}$表示样本 i 对应的特征 j。

每一颗分类回归树都会根据样本输入构造一个输入空间，并在分类前将该空间划分为 K 个子空间（$R_1, R_2, \cdots, R_K$），所以回归树模型可以表示为：

$$f(x) = \sum_{k=1}^{K} c_k I\,(x \in R_k) \tag{3-2}$$

其中c_K为划分后每个空间的输出值，当且仅当$x \in R_k$时$I(x \in R_k) = 1$，否则为 0。选择特征 j 作为分裂特征值，并将 s 作为切分点，以切分点为界可以将样本划分为两个区域：

$$R_1(j,s) = \{x|x^j \le s\}\ and\ R_2(j,s) = \{x|x^j > s\} \tag{3-3}$$

划分后的两个区域分别为决策树的左子树和右子树，其中x^j为分裂后的特征值，x^j小于切分点 s 的数据会被分到左子树，x^j大于切分点 s 的样本被分到右子树。这个样本划

分的过程就是 CART 回归树的基本工作原理。CART 回归树产生的目标函数为：

$$\sum_{x_i \in R_n} (y_i - f(x_i))^2 \tag{3-4}$$

为了求出 j 和 s 的确切值，需要将目标函数做转化，求解如下这个目标函数：

$$\min_{j,s} \left[\min_{b_1} \sum_{x_i \in R_1(j,s)} (y_i - b_1)^2 + \min_{b_2} \sum_{x_i \in R_1(j,s)} (y_i - b_2)^2 \right] \tag{3-5}$$

求解 j 和 s 的确切值可以使用遍历的方法。然后通过计算出的最优(j, s)将样本空间切分成为左右子树，对每个区域重复切分来生长这棵回归树，最终得到一颗回归树。

在每一次迭代中，XGBoost 算法都会学习一个新的函数并拟合上一轮预测的残差，从而逐步提高模型的准确性。经过 K 轮迭代之后，XGBoost 算法会得到 K 棵分类树。在使用集成后的分类器对样本进行预测时，算法会根据样本的特征在每棵树中找到对应的叶子节点，每个叶子节点都会包含一个分数，分数总和就是该样本的预测结果。XGBoost 目标函数可以定义为：

$$Obj = \sum_{i=1}^{n} l(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k) \tag{3-6}$$

目标函数由两部分构成，$l(y_i, \hat{y}_i)$是一个损失函数，用来度量预测值和目标值之间的差异。$\Omega(f_k)$表示决策树的复杂度，充当正则化项。与此同时新生成的分类树需要拟合上次预测产生的残差，所以可以将生成 t 棵树之后的预测分数写成：

$$\hat{y}_i^{(t)} = \hat{y}_i^{(t-1)} + f_t(x_i) \tag{3-7}$$

借助这个式子，可以将目标函数改写为：

$$Obj^{(t)} = \sum_{i=1}^{n} l\left(y_i, \hat{y}_i^{(t-1)} + f_t(x_i)\right) + \Omega(f_t) \tag{3-8}$$

然后我们需要找到能够将上式最小化的f_t，并使用泰勒公式在$f_t = 0$处展开目标函数，处理后的目标函数可以近似写为：

$$Obj^{(t)} \cong \sum_{i=1}^{n} \left[l\left(y_i, \hat{y}_i^{(t-1)}\right) + g_i f_t(x_i) + \frac{1}{2} h_i f_t^2(x_i) \right] + \Omega(f_t) \tag{3-9}$$

在该式中一阶导数部分为：

$$g_i = \partial_{\hat{y}^{(t-1)}} l\left(y_i, \hat{y}^{(t-1)}\right) \tag{3-10}$$

二阶导数部分为：

$$h_i = \partial^2_{\hat{y}^{(t-1)}} l\left(y_i, \hat{y}^{(t-1)}\right) \tag{3-11}$$

正则项部分为：

$$\Omega(f) = \gamma T + \frac{1}{2}\lambda\|w\|^2 \tag{3-12}$$

综合以上各式，XGBoost 模型最终的目标函数为：

$$Obj = \sum_{j=1}^{T}\left[\left(\sum_{i\in I_j} g_i\right)w_j + \frac{1}{2}\left(\sum_{i\in I_j} h_i + \lambda\right)w_j^2\right] + \gamma T \tag{3-13}$$

在该公式中I_j表示分类树中第j个叶子节点对应的数据样本集合，w为叶子节点分数。此时目标函数已经被转换成w的一元二次函数，可是使用顶点公式求解w的最优值。计算结果如下：

$$w_j^* = -\frac{G_j}{H_j+\lambda} \tag{3-14}$$

此时的目标函数公式为：

$$Obj = -\frac{1}{2}\sum_{j=1}^{T}\frac{{G_j}^2}{H_j+\lambda} + \gamma T \tag{3-15}$$

该式也可以称为 XGBoost 模型的打分函数，它可以作为衡量模型结构优劣的指标，打分函数的值越小，说明树的结构越好。因此，可以通过打分函数来评估最佳切分点的位置，Gain 表示切分之后左右子树的目标函数差，差值最大的切分点就是最佳切分点。Gain 的计算公式如下：

$$Gain = \frac{1}{2}\left[\frac{G_L^2}{H_L+\lambda} + \frac{G_R^2}{H_R+\lambda} - \frac{(G_L+G_R)^2}{H_L+H_R+\lambda}\right] - \gamma \tag{3-16}$$

3.2 GRU 概述

门控循环神经网络（Gated Recurrent Unit, GRU）是一种循环神经网络（Recurrent Neural Network, RNN），GRU 可以学习到时间上相隔较远的两条记录之间的依赖关系，可以用于处理时间序列数据。GRU 模型结构如图 3.1 所示。

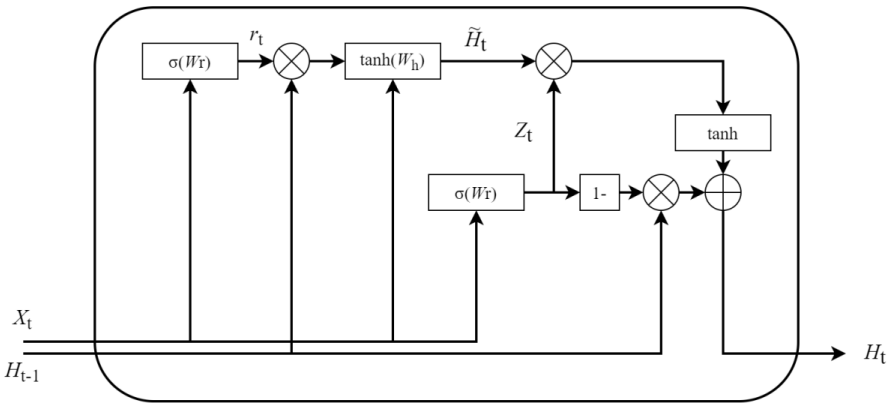

图 3.1 GRU 模型结构图

GRU 的核心思想是通过门控机制来控制信息流的传递。GRU 单元有两个门控单元：重置门（reset gate）和更新门（update gate），以及一个隐藏状态（hidden state）。相关定义如下：

$$R_t = \sigma(W_R X_t + U_R H_{t-1} + b_R) \tag{3-17}$$

$$Z_t = \sigma(W_Z X_t + U_Z H_{t-1} + b_Z) \tag{3-18}$$

$$\widetilde{H}_t = tanh(W_H X_t + R_t \odot U_H H_{t-1} + b_H) \tag{3-19}$$

$$H_t = (1 - Z_t) \odot H_{t-1} + Z_t \odot \widetilde{H}_t \tag{3-20}$$

R_t为重置门，Z_t为更新门，H_{t-1}是上一个时刻的隐藏状态，$\widetilde{H}_t$是当前时刻候选状态，H_t为当前时刻输出的隐藏状态，X_t是当前时刻的输入，σ是 sigmoid 函数用于确定内容是否需要更新，W_R、W_Z和W_H是当前时刻输入的权重参数，U_R、U_Z和U_H是上一时刻隐藏状态的权重参数，b_R和b_Z是偏差参数。

重置门R_t控制当前时刻候选状态$\widetilde{H}_t$是否依赖于上一时刻隐藏状态H_{t-1}，更新门Z_t控制当前时刻状态H_t需要从上一时刻隐藏状态H_{t-1}中保留多少信息，以及需要从候选状态$\widetilde{H}_t$中接受多少新的信息。GRU 通过使用这两个门控来把控数据信息的传递过程，同时也可以凭借该机制学习数据在时间维度上的特有信息，门控单元有效解决了 RNN 在处理长期依赖性序列时出现的梯度消失和梯度爆炸问题。

由于 GRU 只有两个门控单元，对比 LSTM 模型的结构，在设计上更加简单，参数更少，训练速度和效率也更高，并且可以更好地捕捉时间序列中步距较大的依赖关系。

3.3 XGBoost-GRU 模型设计与实现

XGBoost-GRU 模型使用 XGBoost 算法对数据特征进行特征选择，然后对筛选后的低维特征数据做时序化和归一化等预处理，并将处理后的行为数据作为 GRU 神经网络模型输入样本，最终输出行为预测结果。模型结构如图 3.2 所示。

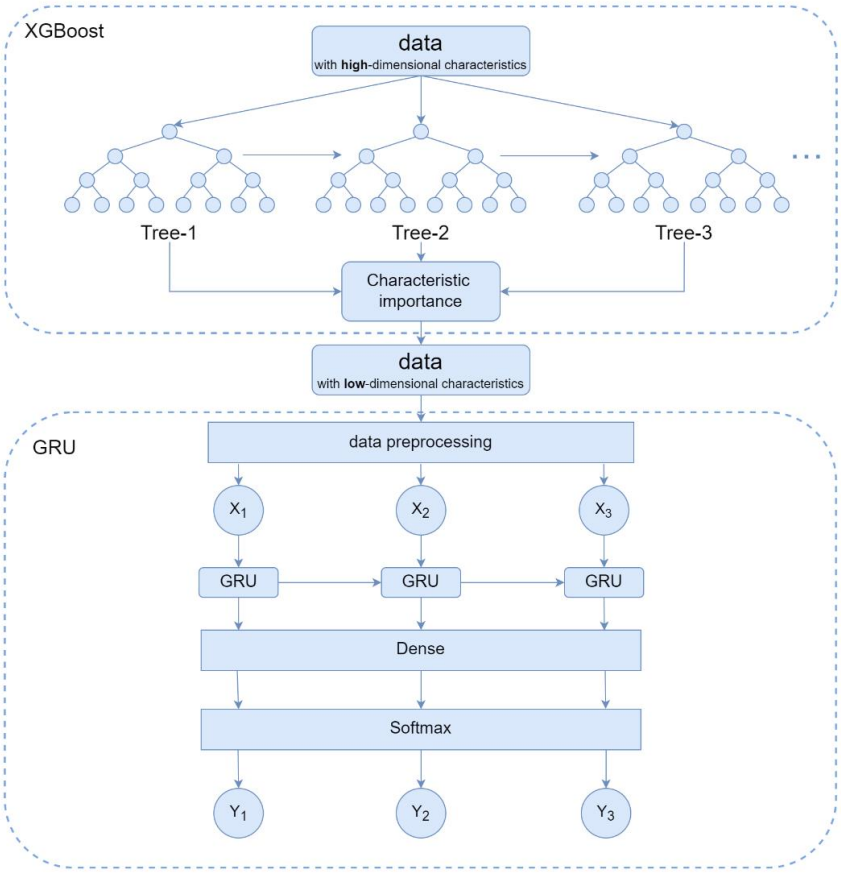

图 3.2 XGBoost-GRU 模型结构图

模型主要分为特征选取和模型训练两个部分。其中，XGBoost 算法负责特征选择，GRU 负责使用降维后的特征数据进行预测，从而达到多分类目的。XGBoost 算法能够在训练结束后得到每个特征的重要性得分，该得分可以衡量特征在模型中对最终预测值的权重，一个特征越频繁的被用于构建决策树，它的重要性得分越高。因此，XGBoost 算法能够高效地输出重要性高的特征，筛选掉部分不重要特征，从而减少特征数量，提高后续模型训练的效率，并减少无关特征对于预测结果的影响。GRU 模型能够学习时间序列中的依赖关系，适用于处理时序数据，相较于 LSTM 更适合处理不太复杂的数据。由于本文选用的数据集包含时序特征，并且通过 XGBoost 算法进行了特征降维，因此 GRU 可以在保证准确率的同时尽可能提高训练和预测的效率。

由于物联网终端设备的性能较弱，在实际应用场景中要尽可能减少设备的负担，所以使用 XGBoost 算法筛选出数量较少的特征用于降低终端采集信息时的负载，借此减少传输数据的长度以提高效率。同时利用 GRU 模型在处理精简数据时优异的性能，比起 LSTM 能够更快训练和输出预测结果，使得 XGBoost-GRU 模型能够适应于物联网环境。

3.3.1 数据集准备

本文采用 Bot-IoT 数据集，由新南威尔士大学网络中心于 2018 年公开。该数据集包含正常流量和僵尸网络流量，用于模拟物联网环境下的正常和恶意访问行为流量数据。原始数据集包含 42 个特征，表 3.1 列出了该数据集的一些特征示例。

表 3.1 Bot-IoT 数据集特征示例

名称	数据类型	描述
pkSeqlID	Guid	序列 ID
stime	Float	记录开始时间
proto	Category	流量协议
Saddr	Category	源 IP 地址
srate	Float	每秒源地址到目标地址的数据包数
mean	Float	记录平均持续时间
Sport	Category	源端口号
…	…	…

入侵事件分为三个不同类别，即端口扫描、拒绝服务（DoS）、分布式拒绝服务攻击（DDoS）。表 3.2 展示了数据集中各类数据的统计情况。

表 3.2 Bot-IoT 数据类型统计

事件	类型	事件数量
正常	正常访问	107
攻击	DoS（52.52%）	385309
	DDoS（44.99%）	330112
	端口扫描（2.48%）	18163
事件总数		733691

为了充分利用数据的时序信息，使用数据集中的记录开始时间字段将样本按照时间序列排序，并对特征进行归一化处理，把数据映射到[0,1]之间。归一化使用公式如下：

$$X' = \frac{x-min}{max-min} \tag{3-21}$$

3.3.2 数据集特征选取

在特征选择之前，为了得到更好的效果，需要对XGBoost算法模型的相关参数调优，XGBoost 模型参数较多，本文选取了一些重要的属性通过网格搜索法和交叉验证进行调参。XGBoost 模型的主要参数如下：

（1）max_depth：分类树的最大深度。通过修改该参数可以调整模型学习局部样本的能力；

（2）learning_rate：学习率，也称为 eta。设置较小的值可以让模型学习次数增加；

（3）min_child_weight：允许叶子节点继续拆分的最小样本权重和。若一个叶子节点的样本权重总和小于该参数就不会继续拆分；

（4）sub_sample：每棵树随机采样的样本比例。可以给该参数设置较小的值来防止过拟合的发生，但是过小的值会增加数据样本拟合偏差；

（5）colsample_bytree：每棵分类树的随机采样的比例；

（6）gamma：叶子节点进行分支时对损失减小的最小要求。该参数越大，模型就趋于保守。

选取 max_depth、learning_rate、min_child_weight、sub_sample、colsample_bytree、gamma 这 6 个参数进行调优，其中各参数调优选值如表 3.3 所示。

表 3.3 XGBoost 模型参数调优范围

参数	调优范围
max_depth	3~25
learning_rate	0.01~0.25
min_child_weight	0.1~0.5
sub_sample	0.6~1
colsample_bytree	0.6~1
gamma	0.05~0.5

网格搜索法会在所有候选参数中，按照设定好的步长依次修改参数的取值，通过枚举每种参数组合情况，找寻所有情况中最佳的参数组合。结果的优劣使用交叉验证进行评估，保证所有数据都能够用于训练和验证，使得评估结果更加可信，同时可以在一定

程度上避免过拟合的问题。网格搜索法输出的最佳参数如表 3.4 所示。

表 3.4 网格搜索法输出结果

参数	输出结果
max_depth	10
learning_rate	0.05
min_child_weight	0.2
sub_sample	0.9
colsample_bytree	0.8
gamma	0.1

使用最佳参数进行模型训练，并根据特征重要性结果选择合适的特征集合进行后续模型训练，本文将在第 3.4 节中将详细描述实验过程。

3.3.3 GRU 模型训练

本文采用 GRU 神经网络进行模型训练和行为检测，该模型由一个输入层、一个 GRU 层、一个全连接层和一个多类预测输出层组成。GRU 层和全连接层的激活函数选用线性整流函数 ReLU，损失函数选用分散交叉熵损失函数，并使用 Adam 优化器进行权重更新，过拟合问题则使用 dropout 技术克服。具体配置信息如表 3.5 示。

表 3.5 GRU 模型配置细节

参数	配置
GRU 层	unit=64
全连接层	unit=16
激活函数	ReLU
dropout	0.2
输出层	Softmax
损失函数	Sparse Categorical Crossentropy
优化器	Adam
训练集和测试集分配	80% and 20% respectively

3.4 模型实验分析

3.4.1 实验环境配置

本节将比较使用不同特征组合的模型性能来确定最终的特征选择结果。在确定最佳特征集合后，使用该集合的特征对模型进行训练和调优。同时，将该模型与其他机器学习模型进行对比，以验证该模型在行为检测领域的良好表现。实验环境配置如表 3.6 所示。

表 3.6 机器学习实验环境配置

配置项	配置环境
操作系统	Windows10 专业版
系统类型	64 位
CPU	Intel Core i7-10750H
GPU	NVIDIA GTX 1660 Ti
编程语言	Python3.10
编程软件	Vistual Studio Code
第三方库	Numpy、Tensorflow、Pandas、Sklearn

3.4.2 性能评价指标

深度学习算法将行为检测转化为多分类问题进行研究。以正常访问行为举例，最终输出结果为：正常行为 P、异常行为 N。模型输出的实际分类结果可以划分为：真正常 TP（True Positive）、假正常 FP（False Positive）、真异常 TN（True Negative）、假异常（False Negative）。表 3.7 为混淆矩阵的相关定义。

表 3.7 混淆矩阵

	实际正常样本 T	实际异常样本 F	
判正常样本 P	TP	FP	判正常样本总数 TP+FP
判异常样本 N	FN	TN	判异常样本总数 FN+TN
	实际正常总数 TP+FN	实际异常总数 FP+TN	

为了从多个角度反映模型的预测性能，采用召回率 Recall、精度 Precision、F1-Score 和准确率 Accuracy 作为模型的评价指标，各性能指标的定义如下：

$$Recall = \frac{TP}{TP+FN} \tag{3-22}$$

$$Precision = \frac{TP}{TP+FP} \tag{3-23}$$

$$F1_{score} = \frac{2*Recall*Precision}{Recall+Precision} \tag{3-24}$$

$$Accuracy = \frac{TP+TN}{TP+FN+FP+TN} \tag{3-25}$$

3.4.3 实验结果评估

实验一：特征选择评估实验

本实验首先使用 XGBoost 模型提取特征重要性，模型的超参数在 3.3.2 小节中通过网格搜索法给出，特征重要性结果如图 3.3 所示。

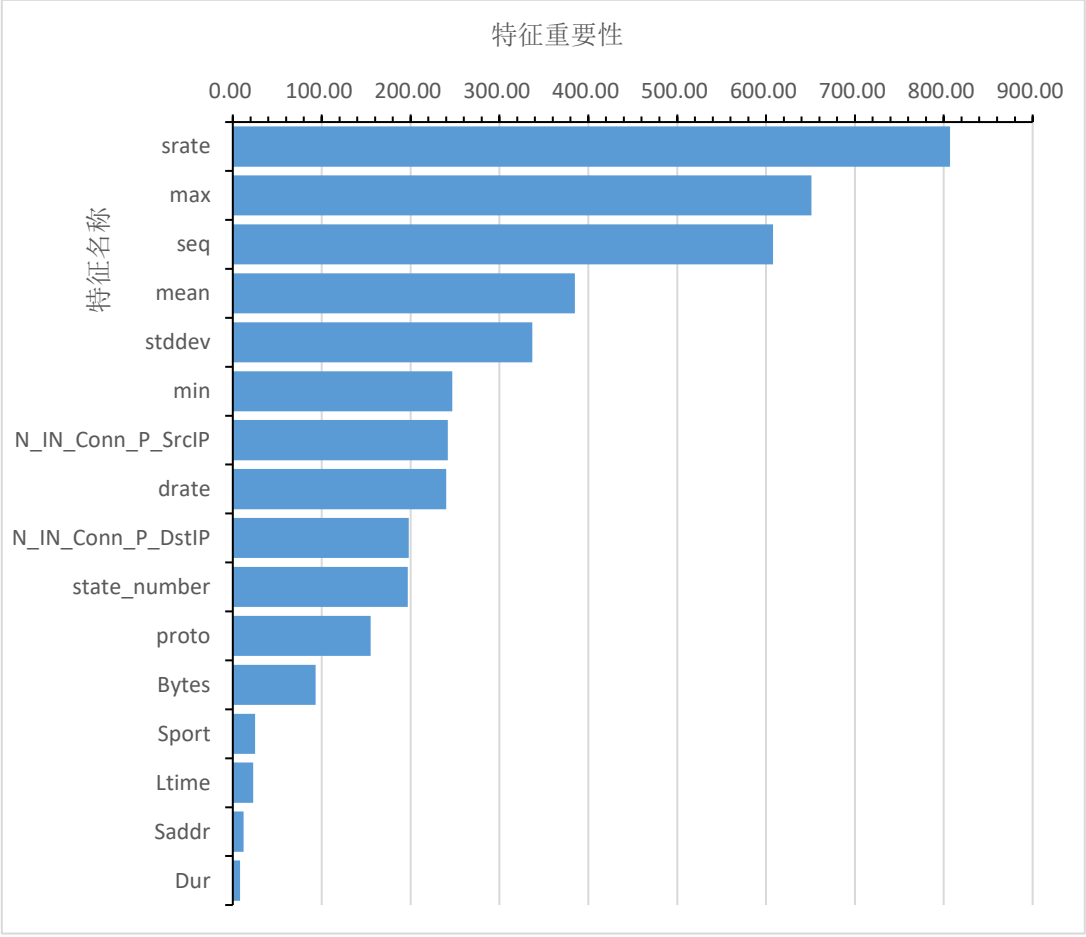

图 3.3 重要性特征分布

图中展示了特征重要性排名前 16 的特征，按照重要性分值从高到低排列，然而这并不是最佳特征集合，接下来使用不同特征集合的数据样本作为 GRU 模型的输入参数，根据模型最终性能指标评估最佳特征集合。选取重要性为前 N 的特征进行模型训练，N 的取值范围为 16~7 之间。训练结束后使用测试集进行测试，最终结果如图 3.4 所示。

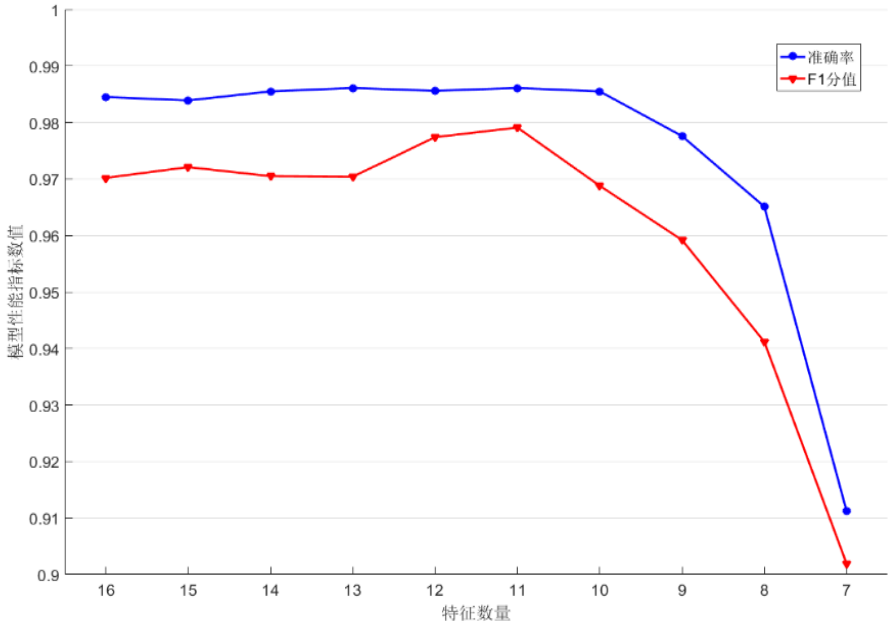

图 3.4 特征数量-性能指标折线图

该折线图趋势表明，XGBoost-GRU 模型的准确率和 F1 分值会随着特征的数量改变而变化。特征数量较多时，不同实验组准确率十分相近，在特征数量为 13 和 11 时最高达到 98.61%，但是 F1 分值会随着特征数量的减少而提高，在特征数量为 11 时达到最大值。特征值数量低于 9 时，由于剩下的特征无法支持模型进行准确预测，准确率会大幅度下降。综合分析可以得出，特征数量为 11 时，该模型的测试效果最佳。最佳特征集合及特征含义如表 3.8 所示。

表 3.8 最佳特征集合

特征名称	含义
srate	每秒源地址到目标地址的数据包数
max	汇总记录中的最大持续时间
seq	流量序列号
mean	汇总记录中的平均持续时间
stddev	汇总记录的标准偏差
min	汇总记录中的最小持续时间
N_IN_Conn_P_SrcIP	源 IP 流量连接数
drate	每秒目标地址到源地址的数据包数
N_IN_Conn_P_DstIP	目标 IP 流量连接数
state_number	事件状态的数字表示
proto	流量协议

实验二：模型性能分析和对比

在选定最佳特征后，通过改变和调整模型的超参数（学习率、epoch、batch_size）数值进行对比实验，以达到最佳训练效果。对比实验结果表明，学习率为 0.001、epoch 为 15、batch_size 为 512 时模型的训练效率和测试结果最为优秀。

模型组合前后性能对比实验结果如图 3.5 所示。

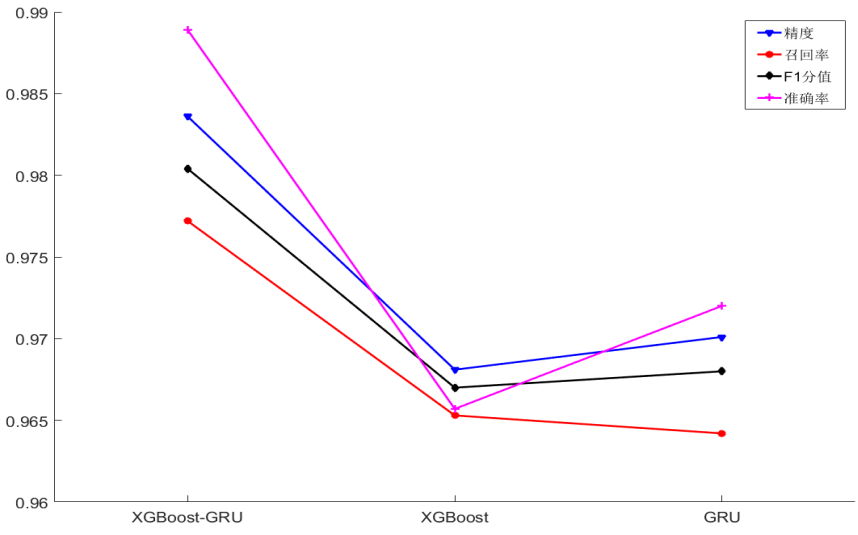

图 3.5 模型组合前后性能对比折线图

使用 XGBoost-GRU、XGBoost、GRU 模型的最佳训练结果进行对比，GRU 模型在准确率和精度方面比 XGBoost 更优，但是 XGBoost 模型的召回率更高。组合前的两个

模型在 Bot-IoT 数据集上已经取得了优秀的预测效果，预测准确率分别达到 96.57%和97.2%。但是，在经过模型组合后，XGBoost-GRU 模型的性能要强于未组合前的单一模型，在精度、召回率、F1 分值、准确率四个方面都要优于 XGBoost 和 GRU，准确率提高到 98.89%。

XGBoost-GRU 模型和其他经典机器学习模型在 Bot-IoT 数据集上的表现如表 3.9 所示。

表 3.9 不同模型性能对比分析表

指标	XGBoost-GRU	LSTM[49]	CNN	Random Forest[50]	KNN
准确率	**98.89%**	98.43%	97.1%	95.04%	93.22%
精度	98.36%	**98.42%**	96.24%	94.43%	91.2%
召回率	**97.72%**	97.46%	97.57%	94.8%	92.43%
F1 分值	**98.04%**	97.93%	96.90%	94.61%	91.81%

从上表结果可以看出，XGBoost-GRU 模型各项性能指标和 LSTM 相近，准确率、召回率和 F1 分值都高于 LSTM，虽然在精度上稍有欠缺，但是比 CNN、Random Forest、KNN 都有明显的优势，证明了本文将 XGBoost 与 GRU 组合设计的合理性和有效性。虽然该模型与 LSTM 的性能差距不大，但是 XGBoost-GRU 模型的训练和预测效率更高，速度更快，能够适应性能较弱的物联网设备，也可以减少应用环境中的检测时延。

3.4.4 实验总结

本文旨在实现零信任架构下物联网设备和用户安全接入云计算服务，所以如何动态检测访问主体的攻击行为变得至关重要。本节通过实验证明 XGBoost-GRU 模型在攻击行为检测领域具有优秀的性能。在实验一中，通过对比不同特征选择下的模型性能，得出最佳特征集合，有效提高了模型的训练效率和预测准确率。实验二将 XGBoost-GRU 模型与其他模型进行性能对比，首先与未组合前的 XGBoost 和 GRU 模型对比，证明模型组合方式的合理性和有效性，然后与其他经典机器学习模型对比，突出本文提出模型的优秀性能。

3.5 本章小结

本章提出了一种基于 XGBoost 算法和 GRU 神经网络的攻击行为检测模型。首先，通过研究 XGBoost 算法和 GRU 神经网络的结构特点和底层原理，解释了将其应用在物联网行为检测领域的合理性。然后设计并实现了该模型，使用 Bot-IoT 数据集对该模型进行训练和测试。在样本数据预处理阶段，根据流量序列号和事件时间将数据样本按照时间序列排序，并对特征进行归一化处理。接着利用 XGBoost 模型的可解释性输出了高重要性特征，并将筛选后的最佳特征样本作为 GRU 神经网络的输入，以提高模型的预测准确性和训练效率。得到模型性能指标后，通过与未组合前的 XGBoost、GRU 模型进行对比，证实了将两者组合后能够提高模型的性能。最后，将性能指标与其他经典机器学习模型（LSTM、CNN、Random Forest 等）进行比较，分析模型的优势。综上所述，本章提出的 XGBoost-GRU 行为检测模型能够为物联网设备和用户提供更可靠和高效的行为检测功能，能够精确预测攻击行为，并用于后续信任值计算。

4 基于访问主体行为的动态信任评估算法

本章引用第三章提出的 XGBoost-GRU 行为检测模型，对信任评估算法展开研究。首先阐述了如何选择和获取访问主体的行为参数，然后提出基于模糊层次分析法的信任评估算法，该算法可以根据行为参数计算访问主体的信任值，并通过引入奖惩机制、时间衰减因子和差异化权重来克服传统信任评估算法的缺点，提高算法的准确性和可靠性。最终通过示例展示信任值计算过程，证明了该算法的有效性。

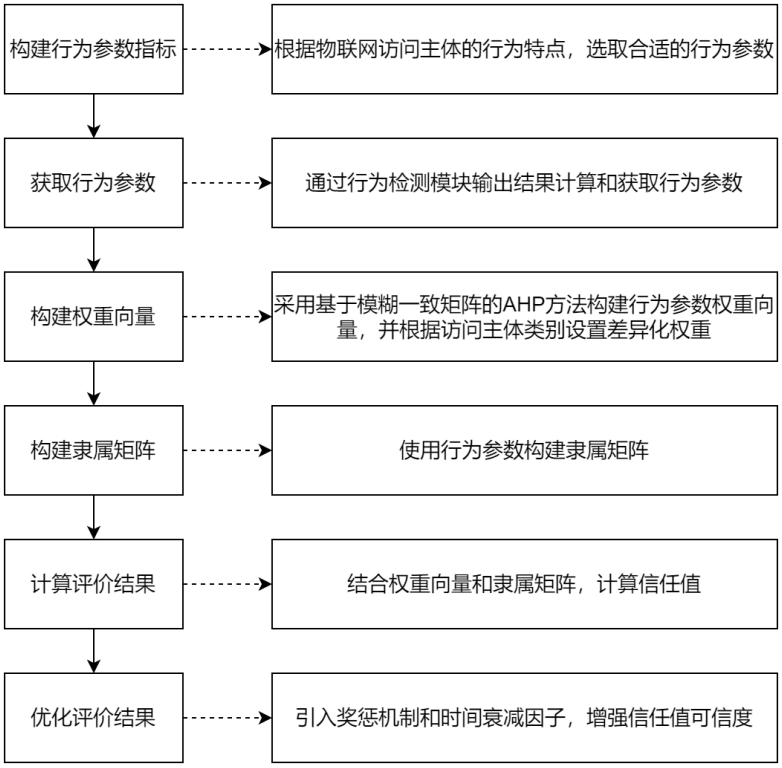

图 4.1 访问主体信任评估流程

图 4.1 访问主体信任评估流程展示了本章设计的信任评估算法的基本流程。首先通过 AHP 层次分析法选取合适的行为参数指标并建立对应的判断矩阵。接着通过行为检测模块获取访问主体行为参数。然后将得到的判断矩阵转换为模糊一致矩阵并计算权重向量。接下来使用收集到的行为参数构造访问主体隶属矩阵，通过权重向量和隶属矩阵计算信任值。最终通过奖惩机制和时间衰减因子更新信任值，使信任值结果可以考虑到历史记录的影响并能够对攻击行为快速做出反应。

4.1 行为参数指标构建

传统的访问控制策略主要使用用户访问凭证来进行身份验证，并决定该次访问是否合法，但是这样的做法存在很多安全隐患。访问凭证可能会被不法分子窃取，访问主体的权限也不能动态调整，而且传统方法难以防护来自网络内部的威胁。一旦访问主体拥有访问凭证，它就可以在系统内部毫无阻拦。而对于一些容易被入侵的物联网设备来说，这个问题无疑十分严重。

为了减少此类情况的发生，就必须摆脱单一的身份认证方法，需要从访问主体多个层面的行为构建行为参数指标，访问凭证只是后续验证的前提条件，访问主体各项行为参数才是信任评估最主要的信任因素。同时，在物联网场景下，需要严格区分用户和设备，并设置差异化的参数权重。用户通常使用移动手机、个人计算机等设备接入云计算服务，这类设备有较强的安全性能，且流动性较大，所以信任评估因素的重点在于访问行为方面。而物联网设备的网络环境基本不会发送变化，且设备安全性较弱，所以要着重于网络行为和攻击行为。但是，不论是设备还是用户，攻击行为层面的因素都占较大比重，设备和用户之间的差异只是相对的。另一方面，访问主体的行为是随时变化的，所以需要通过行为检测模块实时检测，这也是信任评估算法能够动态计算信任值的基础，只有不断分析访问主体的行为，才能实时更新信任值。

行为参数指标可以根据其反映的访问主体相关信息分为两大类：主体相关行为参数和环境相关行为参数。具体参数如图 4.2 和图 4.3 所示。

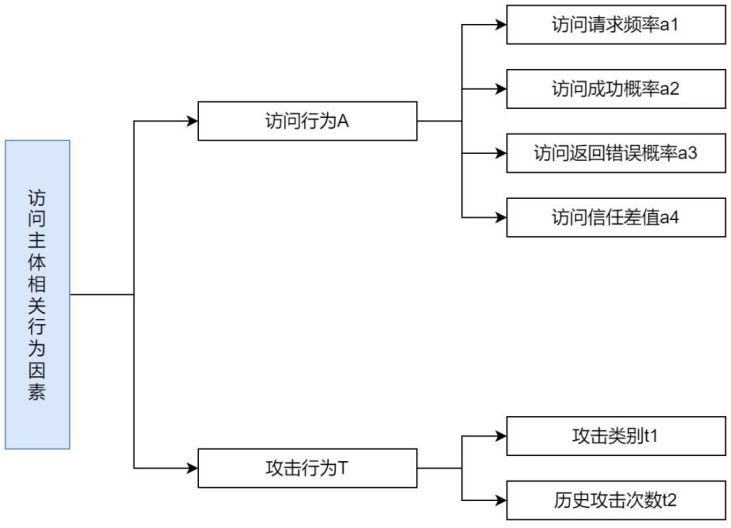

图 4.2 访问主体相关行为因素

访问主体行为参数还可以继续细分，分别为访问行为 A 和攻击行为 T。其中支持访问行为 A 的行为参数包括：（1）访问请求频率 a1；（2）访问成功概率 a2；（3）访问返回错误概率 a3；（4）访问信任差值 a4。攻击行为 T 的行为参数包括：（1）攻击类别 t1；（2）历史攻击次数 t2。

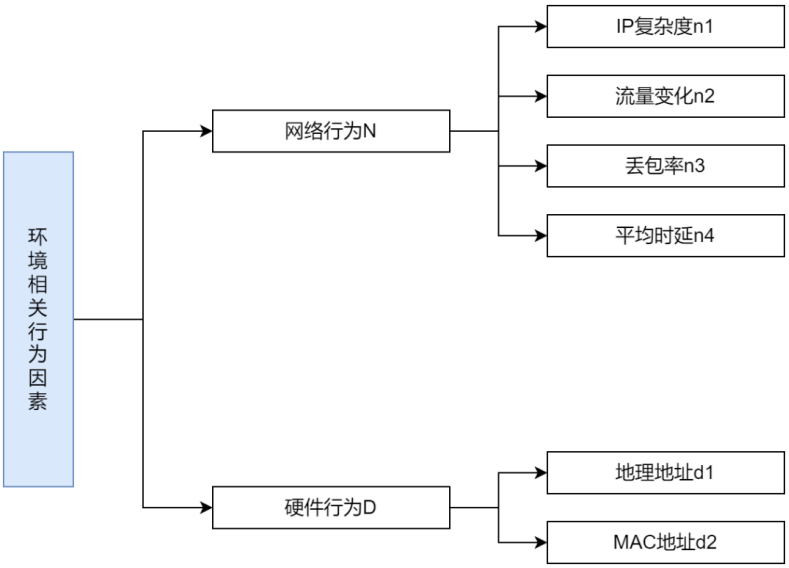

图 4.3 环境相关行为因素

环境相关行为参数也可以继续划分：网络行为 N 是指访问主体发起请求时刻网络相关的环境因素，支撑该属性的证据有以下几点。（1）IP 复杂度 n1；（2）流量变化 n2；（3）丢包率 n3；（4）平均时延 n4。硬件行为 D 是指设备的地理地址 d1 和 MAC 地址 d2。

以上所有的行为参数都是一个 0~1 之间的值，数值越大代表该项行为因素的可信度越高。

4.2 行为参数的获取

行为参数的获取由基于 XGBoost-GRU 模型的行为检测模块采集和预测，并将行为参数存储在行为参数数据库中。行为检测模块的结构如图 4.4 所示。

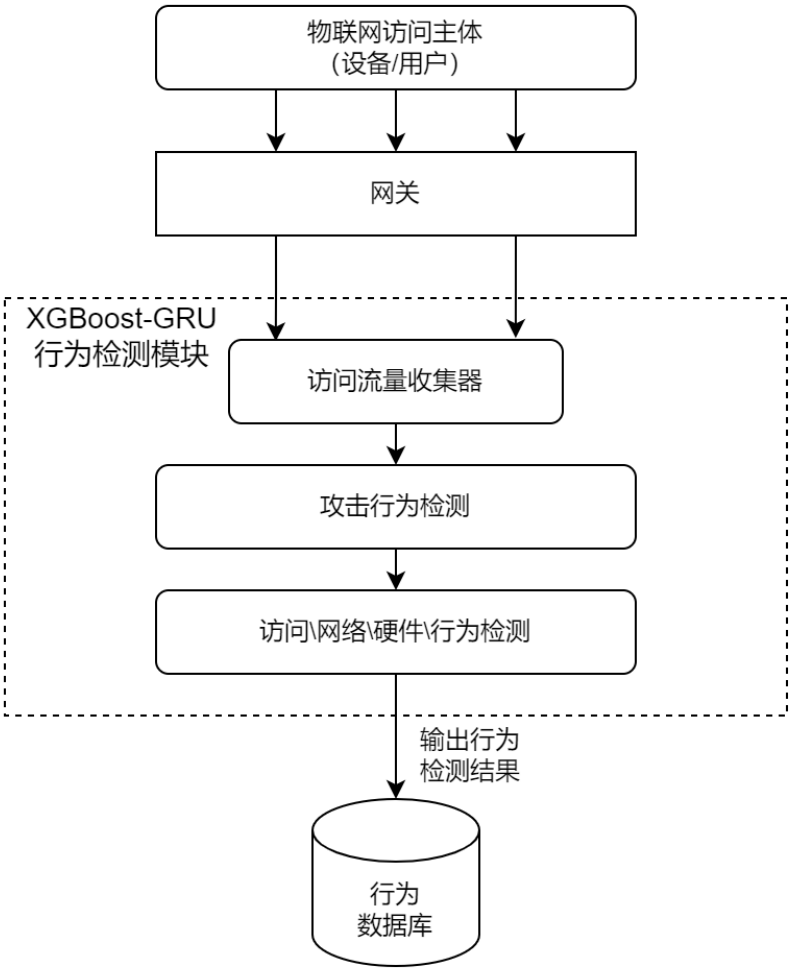

图 4.4 XGBoost-GRU 行为检测模块结构图

XGBoost-GRU 行为检测模块主要有三个组成部分。第一部分是访问流量收集，该流程会将网关中接收到的访问流量进行收集，同时提取访问流量的相关特征（访问流量大小、访问主体 IP 等），在特征完成预处理后传输到后续模块中对行为进行检测。第二部分是攻击行为检测，通过 XGBoost-GRU 模型实现对攻击行为的识别和分类。第三部分是访问\网络\硬件行为检测，该流程会根据本次访问的各项特征，从多个角度评判非攻击行为参数，并计算出对应行为参数的数值。完成检测后系统输出行为检测结果，并将其记录在行为数据库中。

4.2.1 攻击行为参数

攻击行为参数能够反映访问主体是否对系统进行入侵攻击，由于物联网设备易遭受攻击从而被攻击者控制，为了防止攻击者利用被控制的物联网设备进一步对系统进行入侵，零信任信任评估机制必须能够有效阻止攻击行为，所以攻击行为参数是本文提出信

任评估机制最重要的行为参数，同时通过引入 XGBoost-GRU 攻击行为检测模型，凭借其对攻击行为检测的高准确性和可靠性，以确保访问主体安全接入云计算服务。攻击行为参数具体可以细分为以下两种：

（1）攻击行为类别 t1：根据 4.1 节中对攻击行为参数的定义，该模块通过 XGBoost-GRU 模型预测该次访问是否存在攻击行为，并能够检测出具体的攻击种类。攻击的种类对应 Bot-IoT 数据集中的 3 种攻击类别（DDoS、DoS、端口扫描），不同的攻击行为将会体现在该项行为参数中；

（2）历史攻击次数 t2：该项行为参数会根据行为数据库中的历史记录计算同一访问主体的历史攻击次数，次数越多，该项行为参数的分值越低，到达一个阈值之后，该参数分值降为 0。

4.2.2 访问行为参数

访问行为参数能够反映访问主体在请求服务时访问行为的可信程度，在本文信任评估机制中共提出以下四个访问行为参数：

（1）访问请求频率 a1：指访问主体申请访问受保护服务的频率，过低和过高的频率都会影响访问主体的行为评分；

（2）访问成功率 a2：指访问主体成功访问的次数在总访问次数的占比，成功率越高代表行为越好；

（3）访问错误率 a3：指访问主体成功访问之后服务端返回错误次数的占比，该行为参数可以衡量访问主体访问行为的合法性，若某访问主体一直使用错误的参数请求服务，该主体存在安全隐患；

（4）访问信任值差 a4：访问主体每次请求时自身信任值和服务信任阈值差的平均，可以为负数，差值越大说明主体的访问行为越可信。

4.2.3 网络行为参数

网络行为参数能够反映设备网络属性变化的可信程度，共包含以下四个参数：

（1）IP 复杂度 n1：该参数表示用户和设备是如何与云计算服务形成连接，计算该属性需要用到以下定义：

定义 1 IP 树（IP Tree）是一段八位字节，包含所有可能的 IP 地址，需要包含根节点。

定义 2 IP 分支（IP Branch）是一段二阶或三阶的八位字节，包含在此网段下的所有 IP 叶子节点的集合。

定义 3 IP 叶子节点（IP Leaf）指 IP 地址树上的叶子结点，代表一个确定的 IP 地址。

定义 4 IP 扩散（IP Spread）表示所有与该访问主体相关的 IP 树的集合。

定义 5 IP 深度（IP Depth）表示与该主体相关的所有 IP 地址与该主体 IP 分支数量的比值。

访问主体 IP 复杂度计算公式为：

$$d_{ip} = \frac{IP_{Spread}}{IP_{Depth}} \tag{4-1}$$

IP 复杂度可以反映访问主体 IP 地址变化的复杂程度，对于一般的物联网设备，该因素值会较低，因为一般的物联网设备处于一个稳定的网络环境中，一般有固定的 IP 地址，但是对于移动手机等终端设备，IP 复杂度会较高，因为移动手机的 IP 地址会随着用户的地理位置发生改变；

（2）流量变化 n2：表示当前访问与历史窗口上的平均访问流量的方差，用来反映该次访问的网络流量是否异常；

（3）丢包率 n3：表示该主体访问的网络丢包率，反映网络环境是否稳定；

（4）平均时延 n4：表示该主体访问时的平均时延，反映访问请求的速度。

4.2.4 硬件行为参数

硬件行为参数能够反映访问主体的地理位置和设备信息，包含以下两个参数。

（1）地理地址 d1：表示物联网终端的地理位置，大部分物联网设备的地理位置不会发生改变，变化越频繁，该项参数数值越低；

（2）MAC 地址 d2：反映物联网设备硬件在局域网中的唯一性，频繁地变动也会使访问主体的行为变得不可信。

4.3 物联网访问主体信任值计算方法

4.3.1 基于 FAHP 的信任评估算法

在零信任框架中，信任评估算法是最为核心的部分，在获取到行为参数之后，关键的挑战是对计算信任值的各项行为参数设置一个合理的权重分配。本文提出一种基于模糊层次分析法（Fuzzy Analytic Hierarchy Process，FAHP）的信任值评估算法。该算法可以简化评价过程，减少信任值计算的时间，提高访问控制模型的效率。此外文献[52]论证 FAHP 能够很好地模拟人类思维决策过程，具有很好的中分传递性和鲁棒性。

模糊层次分析法是由 Saaty 教授提出的系统分析方法，该算法的特点是在计算过程中将定性和定量的分析方法结合起来，将一些复杂且难以量化的计算转化为可以量化的计算过程。传统的层次分析法有以下几个问题：

（1）难以判断矩阵是否存在一致性；

（2）矩阵不具有一致性时需要多次调整矩阵的元素，使其具有一致性，这个过程需要许多轮调整和检验，缺乏效率；

（3）检验判断矩阵的一致性评判标准科学依据不够充分；

（4）判断矩阵一致性的过程与人类思维的差距较大。

模糊层次分析法在传统层次分析法的基础上，结合模糊一致性矩阵，能够解决上述问题，并且适用于评价指标较多的复杂系统中，和本文研究的问题十分契合。

根据模糊层次分析法的基本原理，需要根据物联网环境和云计算的特点给出影响因素评价指标体系，该体系已于 4.1 小节提出。随后需要选择一个合适的标度法，标度法表示两个行为参数之间重要程度的所有情况，可以表示不同行为参数对于该行为的贡献大小，然后通过该标度法判断矩阵的一致性。本文使用 0.1-0.9 九级标度法，具体如表 4.1 所示。

表 4.1 0.1~0.9 九级度量表

标度	定义	说明
0.1	极端不重要	两元素相比，元素 i 比元素 j 极端不重要
0.2	非常不重要	两元素相比，元素 i 比元素 j 非常不重要
0.3	明显不重要	两元素相比，元素 i 比元素 j 明显不重要
0.4	稍微不重要	两元素相比，元素 i 比元素 j 稍微不重要
0.5	同等重要	两元素相比，元素 i 与元素 j 同等重要
0.6	稍微重要	两元素相比，元素 i 比元素 j 稍微重要
0.7	明显重要	两元素相比，元素 i 比元素 j 明显重要
0.8	非常重要	两元素相比，元素 i 比元素 j 非常重要
0.9	极端重要	两元素相比，元素 i 比元素 j 极端重要

根据度量表和模糊互补矩阵的定义，得到对应属性的判断矩阵，其表示如下：

$$T = \begin{bmatrix} t_{11} & t_{12} & \cdots & t_{1n} \\ t_{21} & t_{22} & \cdots & t_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ t_{n1} & t_{n2} & \cdots & t_{nn} \end{bmatrix}$$

得到判断矩阵之后，根据公式（4-2）和（4-3）转换为模糊一致矩阵。

$$r_i = \sum_{k=1} t_{ik}\ ,\ i = 1,\ 2,\ \cdots n \tag{4-2}$$

$$r_{ij} = \frac{r_i - r_j}{2n} + 0.5 \tag{4-3}$$

再根据公式（4-4）将模糊一致矩阵归一化处理，得到对应的权重向量 W_n，该向量可以表示各信任证据对信任属性的重要程度。

$$w_i = \frac{1}{m(m-1)/2}\left(\sum_{k=1}^{m} t_{ik} - 0.5\right) \tag{4-4}$$

最后将收集到的行为参数规范化处理，得到访问主体初始信任证据矩阵，然后将模糊一致矩阵与初始信任证据矩阵相乘，得到一个新的矩阵。该矩阵对角线上的值就是最终的信任评估向量，用于评估访问主体的信任水平。最后根据公式（4-4）计算出信任属性的权重向量 $\boldsymbol{W_f}$。然后通过公式（4-5）计算访问主体信任值：

$$T = 1 - F \times W_f \tag{4-5}$$

4.3.2 权重向量计算过程

接下来根据 4.2.1 小节给出的计算过程，以访问行为 A 为例，计算权重向量。通过现有的测试数据和测试经验可以得知，访问行为 A 的行为参数重要程度为 $a_2>a_3>a_4>a_1$，由九级标度法可以得到判断矩阵 TQ_A 为：

$$TQ_A=\begin{bmatrix}0.5 & 0.1 & 0.2 & 0.4\\ 0.9 & 0.5 & 0.6 & 0.7\\ 0.8 & 0.4 & 0.5 & 0.6\\ 0.6 & 0.3 & 0.4 & 0.5\end{bmatrix}$$

根据公式（4-2）、（4-3）计算出模糊一致矩阵 TQ_A：

$$TQ_A=\begin{bmatrix}0.5 & 0.3125 & 0.3625 & 0.425\\ 0.6875 & 0.5 & 0.45 & 0.3875\\ 0.6375 & 0.55 & 0.5 & 0.4375\\ 0.575 & 0.6125 & 0.5625 & 0.5\end{bmatrix}$$

然后根据公式（4-4）使用模糊一致矩阵计算出权重向量如（4-6）所示：

$$w_{\mathrm{A}}=\left(0.1833，\ 0.3083，\ 0.275，\ 0.2333\right)^T \tag{4-6}$$

同理，攻击行为 T 的行为参数重要程度为：t1 > t2 判断矩阵 TQ_T 为：

$$TQ_T=\begin{bmatrix}0.5 & 0.8\\ 0.2 & 0.5\end{bmatrix}$$

计算所得的模糊一致矩阵为：

$$TQ_T=\begin{bmatrix}0.5 & 0.65\\ 0.35 & 0.5\end{bmatrix}$$

威胁行为权重向量计算结果如（4-7）所示：

$$w_{\mathrm{T}}=\left(0.65，\ 0.35\right)^T \tag{4-7}$$

同理可得网络行为 N 的行为参数重要程度为：n2>n1>n3=n4，其判断矩阵 TQ_N 为：

$$TQ_N=\begin{bmatrix}0.5 & 0.4 & 0.7 & 0.7\\ 0.6 & 0.5 & 0.8 & 0.8\\ 0.3 & 0.2 & 0.5 & 0.5\\ 0.3 & 0.2 & 0.5 & 0.5\end{bmatrix}$$

计算所得的模糊一致矩阵为：

$$TQ_N=\begin{bmatrix}0.5 & 0.45 & 0.6 & 0.6\\ 0.55 & 0.5 & 0.65 & 0.65\\ 0.4 & 0.35 & 0.5 & 0.5\\ 0.4 & 0.35 & 0.5 & 0.5\end{bmatrix}$$

威胁行为权重向量计算结果如（4-8）所示：

$$w_{\mathrm{N}} = \left(0.275，0.3083，0.2083，0.2083\right)^{T} \tag{4-8}$$

同理，硬件行为 D 的行为参数重要程度为：d2 > d1 判断矩阵 TQ_D 为：

$$TQ_D = \begin{bmatrix} 0.5 & 0.4 \\ 0.6 & 0.5 \end{bmatrix}$$

计算所得的模糊一致矩阵为：

$$TQ_D = \begin{bmatrix} 0.5 & 0.45 \\ 0.55 & 0.5 \end{bmatrix}$$

威胁行为权重向量计算结果如（4-9）所示：

$$\mathrm{w_T} = \left(0.65，0.35\right)^{T} \tag{4-9}$$

再计算访问主体相关行为的权重向量。其重要性 T>A，计算所得的权重如（4-10）所示：

$$w_{\mathrm{B}} = \left(0.45，0.55\right)^{T} \tag{4-10}$$

同理计算出环境相关行为的权重向量，其重要性 N>D，权重向量如（4-11）所示：

$$w_{\mathrm{E}} = \left(0.65，0.35\right)^{T} \tag{4-11}$$

在计算出行为和环境的权重之后，根据测试经验判断，主体相关行为和环境相关行为的信任值权重为$\left(0.7，0.3\right)$。

以上就是在用户访问系统时各属性计算权重向量的过程。由于用户和设备在零信任访问控制模型中是严格区分的，针对物联网设备和用户之间的差异，对于各属性的重要程度也会有区别。所以设置差异化权重，设备访问过程中的权重向量如下所示：

$$w_{\mathrm{B}} = \left(0.35，0.65\right)^{T} \tag{4-12}$$

$$w_{\mathrm{E}} = \left(0.65，0.35\right)^{T} \tag{4-13}$$

对于物联网设备，主体相关行为和环境相关行为的信任值权重度为$\left(0.6，0.4\right)$。这个权重可以有更细粒度的区分，针对不同性能的物联网设备进行特定配置，以实现差异化。通过调整模糊矩阵以及主体相关行为和环境相关行为之间的权重比，该算法可以更加灵活地适应物联网复杂环境，提高其适用性。

4.3.3 信任值的记录和更新

为了更好地考虑历史行为对信任值的影响，本算法引入时间衰减因子和奖惩机制。在计算出当前访问信任值之后，使用滑动窗口记录信任值，当计算出新的信任值之后，所有窗口向后移动一格，并记录下新的信任值。同时根据主体访问的行为，会有一定的奖励或者惩罚。例如，若当次访问产生异常行为，如越权访问、端口扫描攻击等，就会根据滑动窗口中历史记录减少当次访问的信任值；反之，当一个访问主体正常访问系统，该主体的信任值也会不断累积加大。通过这些机制的运用，可以提高信任值计算结果的可信度和鲁棒性。

根据历史行为和时间衰减因子计算更新信任值的方法如下：

公式（4-14）是根据滑动窗口中记录的信任值计算主体信任值的计算公式。

$$T = \sum_{i=0}^{h} \theta(t_i) T_i \tag{4-14}$$

其中 T_i 表示滑动窗口中记录的历史信任值，h 表示窗口大小，$\theta(t_i)$为对应历史信任值的权重。$\theta(t_i)$的表达式如（4-15）所示。

$$\theta(t_i) = \frac{\omega(t_i)}{\sum_{i=1}^{h} \omega(t_i)} \tag{4-15}$$

其中$\omega(t_i)$为时间衰减因子，其表达式如（4-16）所示。

$$\omega(t_i) = \frac{1}{\mu^{t_i}} \tag{4-16}$$

其中μ为预设的参数，取值范围是(1,1.1]，随着t_i的增加，时间衰减因子会减小，相应的信任值权重也会减小，越接近的历史信任值对最终信任值的影响越大，符合信任理论。通过将滑动窗口和时间衰减因子引入信任评估算法中，可以提高该算法的可靠性，使访问控制策略更加安全。

除此之外，为了防止恶意访问主体对云计算资源进行摇摆攻击，即长期进行正常访问以积累信任值后发起重要事务攻击，本文将在算法中引入奖惩机制，具体流程如图 4.5 所示

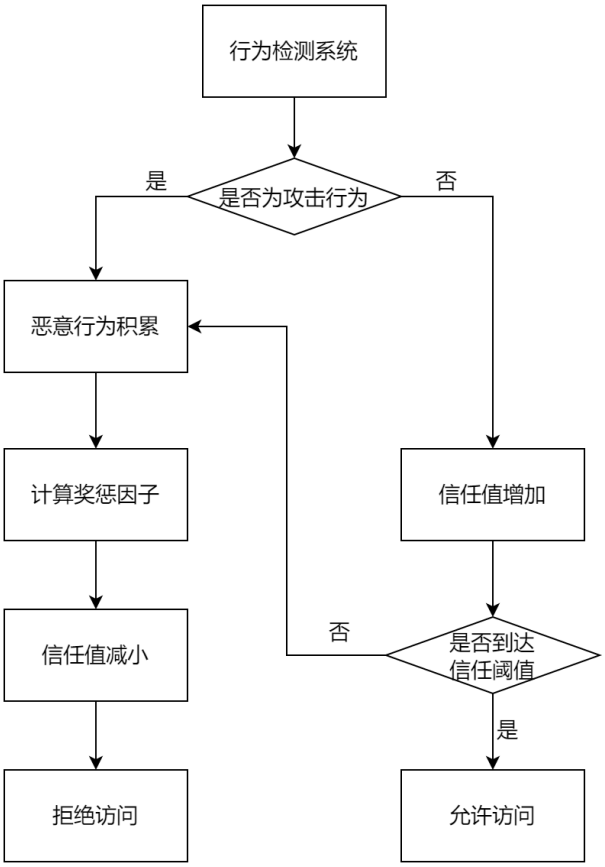

图 4.5 访问主体信任奖惩流程

为了实施奖惩机制，需要借助行为检测模块的结果。首先，该模块会判断当前访问是否为攻击行为。如果是，则记录该恶意行为，并根据行为检测系统的结果，给予相应的惩罚。具体的惩罚方式是根据访问客体的信任阈值计算一个上限值，计算公式如下：

$$p = Csin(\frac{r}{2R} \times \pi) \times T \tag{4-17}$$

其中 T 为访问客体所需的信任阈值，C 为惩罚系数，R 为攻击行为最高等级，r 为访问主体攻击行为等级。当检测到当前访问为攻击行为时，最终信任值为算法所得信任值和 p 中较小的一方，以确保访问会被拒绝。若下次再检测到同一访问主体的攻击行为，阈值会在上次计算所得惩罚的基础上再次进行惩罚。奖励机制体现在，若某一个访问主体长时间正常访问，会在访问行为层面提高行为参数的数值大小，从而提高信任度。

本算法通过引入奖惩机制和时间衰减因子，充分考虑了历史访问行为对信任值计算的贡献，能够对攻击行为做出更快速的反应，迅速降低恶意访问主体的信任值，提高算法灵敏性。

4.4 信任值计算过程

实验数据根据 BotT-IoT 数据集中的数据进行构造，挑选测试数据集中的不同行为参数构造不同种类访问主体，如正常设备的所有访问行为都为数据集中的正常行为数据，恶意设备则会加入攻击行为。一个初始设备的证据数值如下：

$$E_A = (0.6，0.6，0.5，0.6)$$

$$E_T = (0.9，0.6)$$

$$E_N = (0.6，0.7，0.5，0.5)$$

$$E_D = (0.5，0.7)$$

根据证据层的证据数据和权重向量，按照公式$E_i * w_i$计算所得结果如下：

$$F = \begin{bmatrix} 0.599 & 0.86 \\ 0.558 & 0.501 \end{bmatrix}$$

在根据属性层的权重向量（4-9）、（4-10）。与上述结果计算所得访问行为和访问环境的可信程度分别为：

$$F' = [0.769 \quad 0.538]$$

最后再根据物联网设备的访问行为和环境信任值权重（0.6,0.4）计算所得最终设备信任值为：

$$T = 0.677$$

根据测试经验以及算法特性，将信任值分为表 4.2 所示区间，分别代表访问主体的可信度。

表 4.2 信任值等级区间

信任等级	说明	区间
1	非常不可信	(0.00，0.15]
2	不可信	(0.15，0.3]
3	一般可信	(0.3，0.6]
4	基本可信	(0.6，0.7]
5	比较可信	(0.7，0.85]
6	非常可信	(0.85，1.00]

根据信任值计算结果，可以将访问主体大致分为以上六个信任等级，初始用户计算

所得的信任值 T=0.677，可以判断初始用户的信任等级为基本可信。

4.5 本章小结

本章通过改进模糊层次分析法，提出基于访问主体行为参数的动态信任评估算法，该算法通过引入奖惩机制、时间衰减因子、差异化权重等手段，提高计算结果可信度。本章按照行为参数指标构建、行为参数获取、信任值计算、信任值更新的流程详细描述本算法。随后通过示例计算出初始用户的信任值，给出了信任等级划分依据。该算法将应用于第五章的 BD-ZTBAC 模型，以确保访问控制模型能够准确进行权限把控，验证算法性能和应用于 BD-ZTBAC 模型整体效果的相关实验将于 5.4 小节详细阐述。

5 物联网可信接入访问控制模型的设计与验证

针对物联网设备接入云计算服务的内外网络安全风险，本文选择零信任架构作为访问控制模型的基础框架，并且考虑到物联网环境的特点、设备规格的多样性，提出了BD-ZTBAC 模型。

5.1 模型的相关定义

BD-ZTBAC 融合了零信任思想，将信任值与传统基于属性的访问控制模型相结合，来达到访问控制的目的。来实现更加安全和细粒度的访问控制。

本文基于美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）发布的关于 ABAC 标准文献[51]和《零信任架构》[44]，并结合物联网环境的特点，对 BD-ZTBAC 模型做出如下定义：

定义 6 BD-ZTBAC 模型的形式定义有五个组成部分，分别为主体（Subject，S）、客体（Object，O）、权限（privilege，P）、环境（Environment，E）和信任（Trust，T）。

主体（S）表示访问主体，在本模型中为接入云计算服务的物联网设备和用户。主体属性（SA）包括常规属性和信任属性，其中常规属性包含访问主体的类型、用户名、密钥等。信任属性指代用于计算信任值的各类行为参数，包括与访问主体本身相关的行为参数。

客体（O）指可能被访问主体申请访问的实体。本文提出模型中的客体主要是物联网设备和用户尝试接入的云计算服务资源，主要表现形式是服务接口。客体属性（OA）在本文中指代服务接口的相关属性如路径、IP、信任阈值等。

信任阈值（TT）能够成功访问客体的最低信任值要求。

权限（P）表示主体能对客体可能进行的合法访问行为集合，在本文中权限决定主体是否可以访问客体。

环境（E）指主体访问发生时候的环境和系统相关影响因素，环境属性（EA）在本文中指代与环境因素相关的行为参数。

信任（Trust，T）是指访问主体在特定环境下，对访问客体是否能够按照预期或事先定制好的策略进行安全、可靠访问的可信赖程度。

策略（Policy）是指授权算法的集合。定义在具体环境条件和信任属性下主体是否能够访问客体。本课题中的策略主要依据主体的信任值和客体的信任阈值来进行授权。

物联网环境下基于零信任的云计算访问控制模型架构如图 5.1 所示。

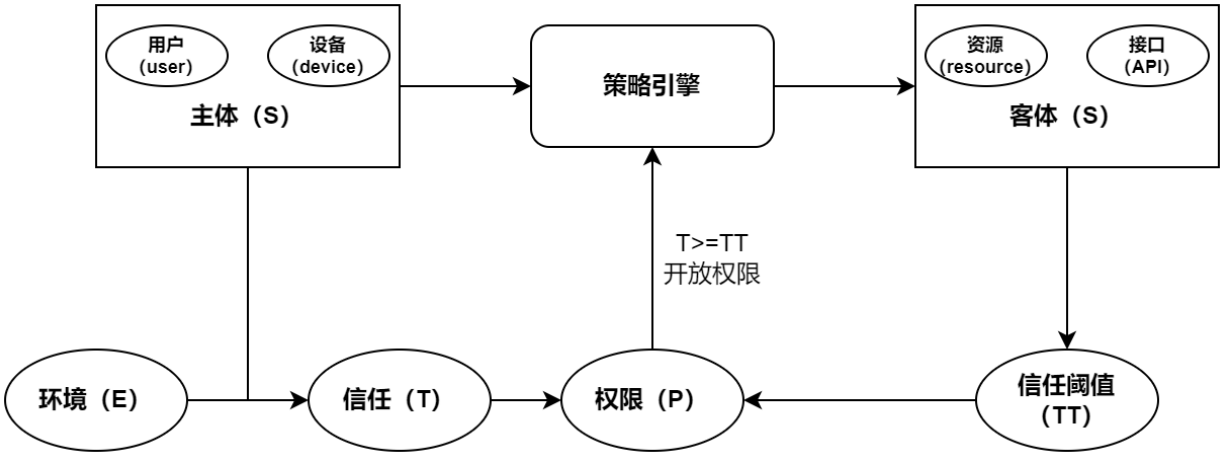

图 5.1 基于零信任的访问控制模型架构图

5.2 模型的访问控制流程

云计算系统主要应用于开放且复杂的网络环境中，再加上物联网设备安全性能弱，极易受到入侵等因素影响，所以在物联网设备和用户接入云计算系统时，默认所有设备和用户都是不可信的。因此要根据访问主体的行为进行分析，对攻击行为快速做出反应并采取对应的访问控制手段，防止恶意访问主体对受到保护的云计算资源造成更多损失。

5.2.1 访问控制组成架构

使用图 5.1 所示访问控制模型架构图，结合第二章给出的零信任组成部分结构图，得出的详细组成架构如图 5.2 所示。

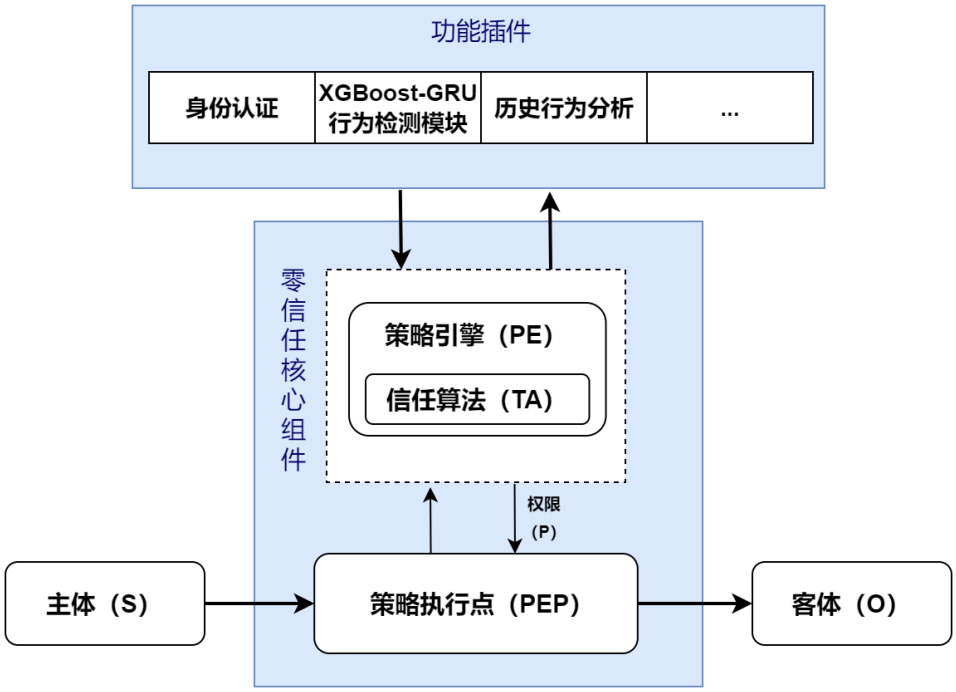

图 5.2 访问控制方法框架图

在该框架中，策略引擎、策略执行点和信任算法为核心部分，该部分包含了信任值计算和访问控制算法。访问主体的请求先到达策略执行点，随后执行点将访问的相关数据上传至策略引擎，同时功能插件对访问主体的相关行为属性进行检测、分析、记录，策略引擎根据功能插件输出结果，使用本文第四章提出的信任评估算法计算出信任值，再通过将信任值和客体信任阈值比较，决定是否授权此次访问，最后将决策结果返回给策略执行点，执行点根据该决策结果执行相应的操作。

除了核心组件之外，功能插件的选择和设计也十分重要。功能插件能够提供信任算法所需的数据，比如身份认证结果、行为检测结果、历史行为分析等。这些插件需要根据云计算和物联网环境的特点进行筛选和评估，因为功能插件的选择往往决定了信任算法是否准确。本文提出访问控制模型的功能插件中包含 XGBoost-GRU 行为检测模块，以提高访问控制模型对攻击行为的抵御能力。

5.2.2 服务授权流程

当访问主体尝试访问受保护的云计算资源时，需要提供信任评估所需要的所有信息。一次完整的访问请求流程如图 5.3 所示，核心代码见算法 5.1。

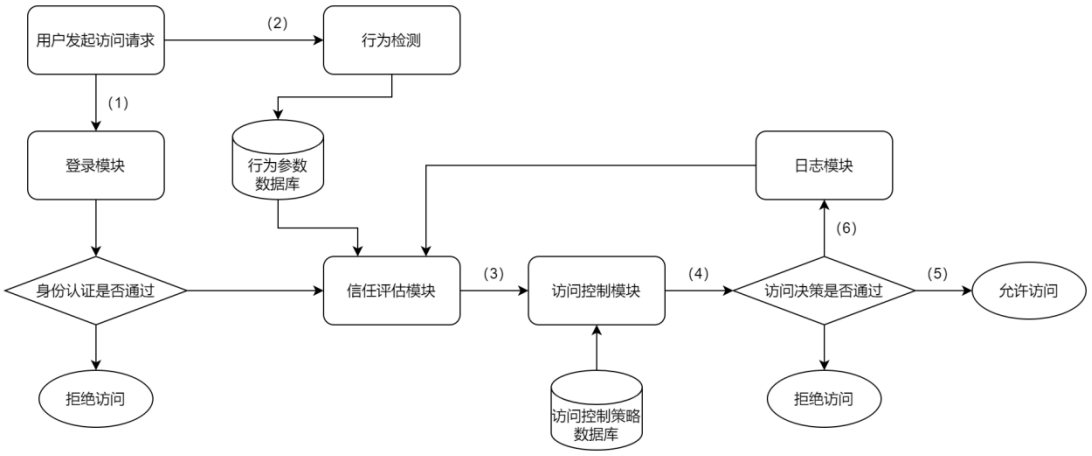

图 5.3 访问控制方法流程图

算法 5.1 访问控制核心算法

输入：访问请求 REQ = (SA,OA,EA)

输出：访问控制决策结果 Decision = (Permit/Deny)

```
BEGIN
1：Decision = Deny          //决策初始化，默认为拒绝访问
2：while REQList.Empty() do       //遍历访问请求队列
3：        REQRecrod = REQList.Get()
4：        if IdentityAuth (REQrecord) then        //身份认证
5：                BParams = BehaviorDetection (REQrecord)       //行为检测
6：                TrustValue = TrustAlgorithm (REQrecord, BParams)     //信任值计算
7：                Decision = PolicyMatch(REQrecord, TrustValue, BParams)
                   //读取客体对应策略，判断访问是否合法
8：        Log(REQrecord, TrustValue, Decision, BParams)     //记录访问结果
9：  end
10：return Decision //返回最终判定结果
END
```

核心算法详细描述如下：

（1）收到访问主体的请求后，首先会对其进行身份认证，通过登录模块判断用户名和密钥是否正确。若身份认证不通过，直接拒绝访问；若通过则将主体数据做相应处理并发送到信任评估模块；

（2）用户发起访问请求的同时，会将该请求的相关信息发送到行为检测模块，用于检测是否存在攻击行为，并输出行为参数到行为参数数据库；

（3）信任评估模块收到经过处理的访问主体数据后，会从行为参数数据库读取检测结果，并根据结果计算出该主体本次访问的信任值。信任值的计算不仅考虑本次访问的情况，还会通过日志模块参考同一设备或用户历史访问记录，同时结合奖惩机制更新信任值，并将最终的信任值结果传输到访问控制模块；

（4）访问控制模块收到信任值结果和访问主体属性之后，通过访问控制策略数据库查询访问客体对应的信任阈值，再根据信任值比对来决策是否允许该次访问；

（5）若信任值达到访问所需的阈值，则允许访问，同时将此次访问的时间、用户名、信任值和访问结果等相关参数记录到日志模块中用于下次计算行为参数时使用；

（6）若信任值没有达到访问所需阈值，则拒绝访问，并作为恶意访问记录在数据库中。

5.2.3 访问主体行为信任评估流程

在整个访问控制模型中，信任评估模块是核心组件。该模块等于是整个系统的大脑。信任评估流程是否科学规范将能够决定信任值结果是否可信。在本课题中，信任评估流程主要分为图 5.4 中所示的几个阶段。

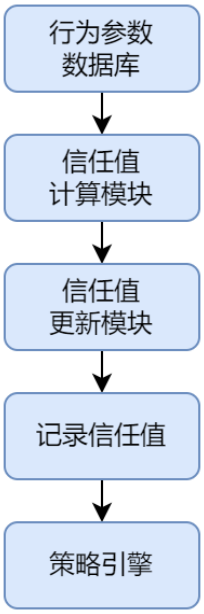

图 5.4 信任评估流程示意图

信任评估模块由三个子模块组成：

（1）信任值计算子模块：基于行为参数数据库中的数据，使用第四章提出的动态信任评估算法计算信任值；

（2）信任值更新子模块：根据访问主体的历史行为计算时间衰减因子和奖惩系数，并将更新后的信任值作为最终结果输出；

（3）信任值记录子模块：将更新子模块更新后的结果记录在历史日志中，用作下次评估的历史记录。

5.3 模型综合分析

通过将 BD-ZTBAC 模型与多个经典访问控制模型对比，结合第二章中得出的访问控制模型评判指标对该模型进行分析。给出以下性能评价，如表 5.1 所示。

表 5.1 访问控制模型性能综合对比分析

模型	有无奖惩机制	支持时间属性	适用于云计算	适用于物联网	授权灵活性	异构性	可拓展性	模型安全性
ABAC	无	不支持	不适用	不适用	中	中	高	低
GTRBA	有	支持	适用	不适用	高	低	高	中
LRBAC	有	不支持	不适用	不适用	中	低	高	低
ARBAC	无	支持	适用	不适用	低	中	中	低
UCON	无	不支持	使用	不适用	高	中	高	高
CT_ABAC	有	不支持	适用	不适用	高	高	高	中
MTRBAC	有	不支持	适用	不适用	高	高	高	低
BD-ZTBAC	**有**	**支持**	**适用**	**适用**	**高**	**高**	**中**	**高**

通过上表的对比可以看出，BD-ZTBAC 模型的各项性能指标上表现良好，唯一需要注意的是在可拓展性方面，由于引入了行为检测模块，系统的拓展方面会比较复杂。但是也正是由于引入了该模块，模型安全性能有极大提高，同时能够更好地适应物联网复杂环境。并且本课题中的行为检测模块使用机器学习技术，使其在动态性、灵活性等方面与传统模型比起来都有很大的突破。

5.4 仿真实验分析

为了证明本章提出的 BD-ZTBAC 访问控制模型的效果，本小节通过仿真测试系统对第四章提出的信任评估算法和模型的功能和性能进行验证，由于行为检测模型相关实验已于 3.4 小节展示和分析，所以本章侧重于行为检测模型、信任评估算法和访问控制模型三者结合后的整体性能分析，证实信任评估算法优势和访问控制模型的稳定性。

5.4.1 仿真系统设计

图 5.5 展示的是实验使用的仿真测试系统架构图，包括应用层、支撑层、数据层、数据源与基础设施。

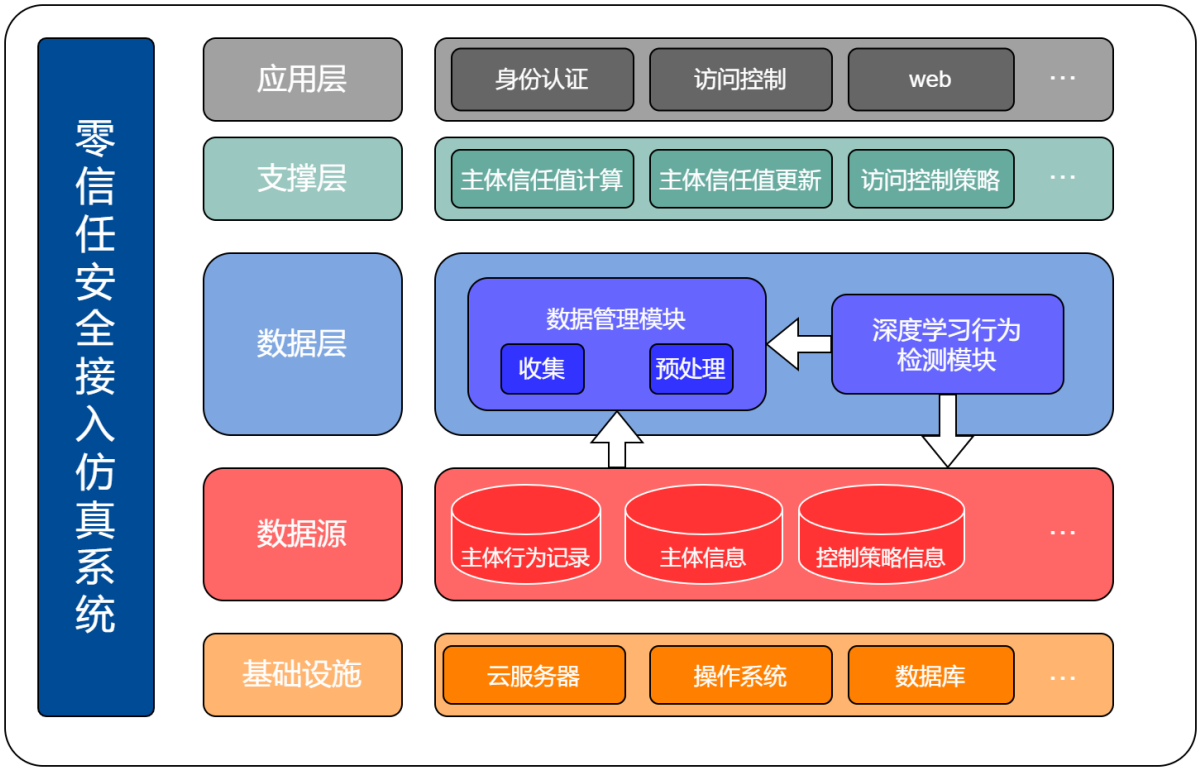

图 5.5 仿真测试系统架构图

其中，应用层主要是提供身份认证、访问控制的接口，同时通过 web 应用方便仿真测试时查看日志和访问主体信任值变化情况。支撑层主要是实现访问主体信任值计算和更新，同时实施访问控制策略。数据层主要是完成数据的收集和预处理，同时通过深度学习行为检测模块检测攻击行为。数据源主要是行为数据库、访问主体信息数据库、访问控制策略数据库等数据存储模块。基础设施包括云服务器、操作系统和数据库，云服务器使用阿里云提供的云服务器，操作系统为 Ubuntu，仿真测试软件系统采用 Vue 作为前端模板框架；Spring Boot、Mybatis 为后端基础框架；使用 MySQL 数据库用于数据存储。这些技术和系统框架均是当下云服务流行的框架，用以最大限度模拟真实环境。研究人员可以通过该系统的前端页面便捷查看各访问主体的信任值变化趋势和访问日志，并可以对云服务 API 进行管理。仿真测试系统的部分截图如图 5.6 所示。

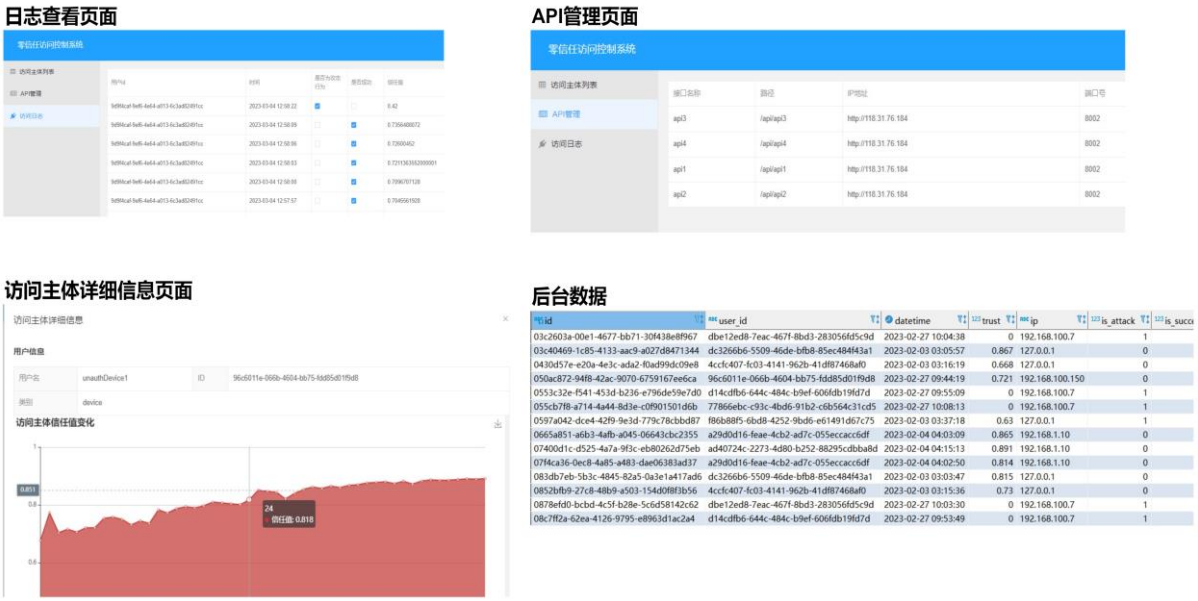

图 5.6 仿真系统部分截图

该系统作用是将行为检测模块、信任评估算法、访问控制模型三者结合，模拟物联网设备和用户接入云计算服务场景，从整体的角度对其进行实验和测试，验证 BD-ZTBAC 模型的访问控制性能。

5.4.2 实验环境配置

本章实验的硬件环境和软件环境如表 5.2 和表 5.3 所示。

表 5.2 实验硬件环境配置

参数\设备	PC 机	云服务器
操作系统	Windows10 专业版	Ubuntu 20.04.1
系统类型	64 位	32 位
服务商	/	阿里云
内存	16GB	4GB

实验将访问控制模型和信任评估模型部署在 PC 机上，受保护的云计算服务接口和数据库部署在阿里云服务器上。

表 5.3 实验软件环境配置

参数\系统名称	BD-ZTBAC 访问控制系统	XGBoost-GRU 行为检测检模型
编程语言	JAVA8、JavaScript	Python3.10
基础框架/库	SpringBoot、Vue	Sklearn、Numpy、Pandas、Tensorflow
数据存储	MySQL	MySQL

软件环境配置方面，访问控制系统相关的程序由 JAVA 编写，使用 SpringBoot 框架，实现对访问的访问控制流程。行为检测模型使用 Python 编写和训练，训练完成之后，再由 JAVA 程序通过 Tensorflow 库的相关 API 调用。

5.4.3 实验数据获取

为了模拟真实环境，实验数据需要构造不同行为属性的用户和设备。用户和设备的每次访问行为都是基于 Bot-IoT 数据集构造，正常用户和设备的行为和属性从数据集正常分类中筛选，恶意用户和设备的行为和属性会在正常分类的基础上混合其它入侵行为的数据。在每次用户和设备访问结束后，会将本次访问记录在数据库中，用作下次信任评估时的历史行为数据。仿真实验所需要的模拟访问主体行为组成如表 5.4 所示。

表 5.4 模拟用户设备行为组成示例

用户/设备种类	访问频率	行为组成
正常设备/用户	20 次/h	100%正常访问
越权访问设备/用户	20 次/h	70%正常访问 30%越权访问
端口扫描攻击设备/用户	20 次/h 攻击时 40 次/h	70%正常访问 30%端口扫描
DoS 攻击设备/用户	20 次/h 攻击时 120 次/h	60%正常访问 40%DoS 攻击
DDoS 攻击设备/用户	20 次/h 攻击时 240 次/h	60%正常访问 40%DoS 攻击

访问主体种类共分为 12 类，每一类访问主体都由不同的访问行为组成，存在攻击行为的访问主体在攻击时，访问频率也会相应提高以模拟真实入侵环境。攻击行为的相关参数来自于 Bot-IoT 测试集对应类别的样本。该表内容只是一个示例，具体的访问频率

和行为组成会视具体实验要求做适当修改。

5.4.4 实验内容设计与目标

仿真实验从奖惩机制、差异化参数权重和时间衰减因子在信任评估算法中的作用入手，对比传统信任评估方法，突出本文提出算法的创新和优秀性能，最后将算法结合到BD-ZTBAC 模型中综合评判模型的功能和性能，实验设计如表 5.5 所示：

表 5.5 访问控制模型实验设计

实验	实验内容	实验目标
实验一	本实验将构造五个不同行为的访问主体，分别为正常设备、越权访问设备、恶意设备（端口扫描）、恶意设备（DoS 攻击）和恶意设备（DDoS 攻击）。这五个设备会向云计算资源发起访问，初始信任值为 0.677。前 14 次为正常访问，从第 15 次访问开始，进行对应的异常访问行为。本实验将会比较五个设备的信任值变化趋势，并与无奖惩机制的情况进行对比。	验证本文所提出的信任评估算法引入的奖惩机制的有效性。
实验二	本实验会构造 1 个物联网设备和一个物联网用户作为本实验的访问主体，同时赋予它们相同的初始信任值。接着它们会对资源进行访问，每次访问逐步减少网络行为参数和硬件行为参数的数值。记录两者的信任值改变趋势，并加以分析。	验证本文提出的信任评估算法可以根据访问主体类别动态分配行为参数权重，做针对性信任计算。
实验三	本实验将构造两组物联网设备。第一组包括两个设备，初始信任值均为 0.89，在有时间衰减因子和无时间衰减因子的情况下进行相同行为的访问，其中包含越权访问行为和正常访问行为，记录两个设备的信任值随访问次数的变化。第二组包括两个设备 A 和 B，它们有相同恶意行为比例的历史访问日志，但是这些日志距离当前访问的时间跨度不同，记录两个设备的信任值随访问次数的变化。	验证本文提出的信任评估算法在时间衰减因子的作用下，相较于传统 AHP 算法，具有更好的时间衰减性和抗攻击性。
实验四	本实验共构造 50 个物联网访问主体，其中设备 25 个，用户 25 个，再根据访问行为细分为五类（正常、越权访问、端口扫描、DoS、DDoS），每类访问主体数量为 5 个，通过自动化测试脚本，在 24 小时内持续访问云计算资源，计算访问控制模型相关性能指标并加以分析。	验证本文提出的访问控制模型能够满足物联网场景下的需求，并且有优秀的性能。

5.4.5 实验结果及分析

实验一：验证本文提出的信任评估算法使用的奖惩机制的有效性

构造不同访问主体对同一云服务接口进行不同行为的访问，访问前期都为正常访问行为，从 15 次开始出现异常行为，图 5.7 是程序输出的部分访问主体信任值计算结果：

正常访问行为设备

```
userName:normalDevice
accessFre:0.64,successFre:0.808,failreturnFre:0.612,trustDiff:0.9
threatenLevel:1.0,unauthNum:0.616
ipCom:1.0,trafficDiff:1.0,packetLoss:0.516,averageDelay:0.9
area:1.0,mac:0.9
trust:0.77375762
```

攻击行为设备

```
userName:dosDevice
accessFre:0.8976,successFre:0.13599999999999998,failreturnFre:0.6539999999999999,trustDiff:0.6
threatenLevel:0.2,unauthNum:0.6048
ipCom:1.0,trafficDiff:1.0,packetLoss:0.5720000000000001,averageDelay:0.9
area:1.0,mac:0.9
trust:0.42
```

越权行为设备

```
userName:unauthDevice
accessFre:0.64,successFre:0.808,failreturnFre:0.612,trustDiff:1.0
threatenLevel:1.0,unauthNum:0.616
ipCom:1.0,trafficDiff:1.0,packetLoss:0.516,averageDelay:0.9
area:1.0,mac:0.9
trust:0.77865692
```

图 5.7 信任值计算程序输出结果

将五个不同类别访问主体信任值记录，随访问次数变化结果如图 5.8 所示。

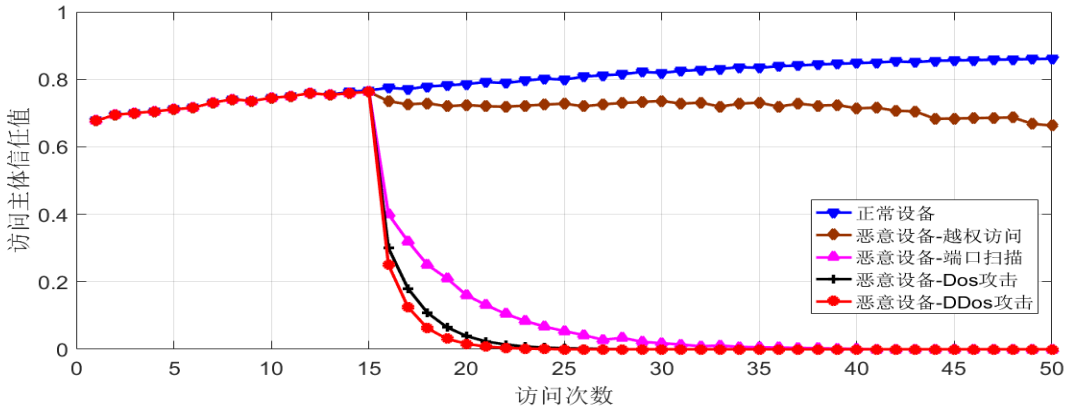

图 5.8 不同访问主体信任值变化趋势

根据图中结果可以分析得出，在第 15 次访问之后，不同设备的信任值呈现不同的变化趋势，正常设备的信任值随着正常访问次数的增加而逐渐提升，最终达到非常可信的信任等级。越权访问设备则会缓慢降低信任值，最终信任等级会降到一般可信的水平。由于越权访问的性质并不是非常恶劣，一些正常的设备和用户也难免会有误操作，因此该行为的惩罚因子设置较小，使得信任值下降的幅度不会过大。剩下的三个恶意设备的

访问行为已经达到攻击级别，其信任值下降的趋势与越权访问设备有显著差异。由于奖惩机制的存在，攻击行为发生的访问主体会受到惩罚，使得这些访问主体的信任值迅速下降，最终访问被拒绝。如果该设备持续入侵，则信任值会在前一次入侵的基础上再次下降，最终信任等级会降至非常不可信。此外，不同的入侵方式也会导致信任值下降的幅度有所不同，幅度取决于攻击的严重程度。因为 DDoS 攻击是三类攻击行为中危害最大的，所以惩罚因子最大，信任值下降的速度最快。接下来本实验将对比有无奖惩机制对访问主体信任值变化趋势的影响，图 5.9 展示的是奖惩机制有效性实验结果图。

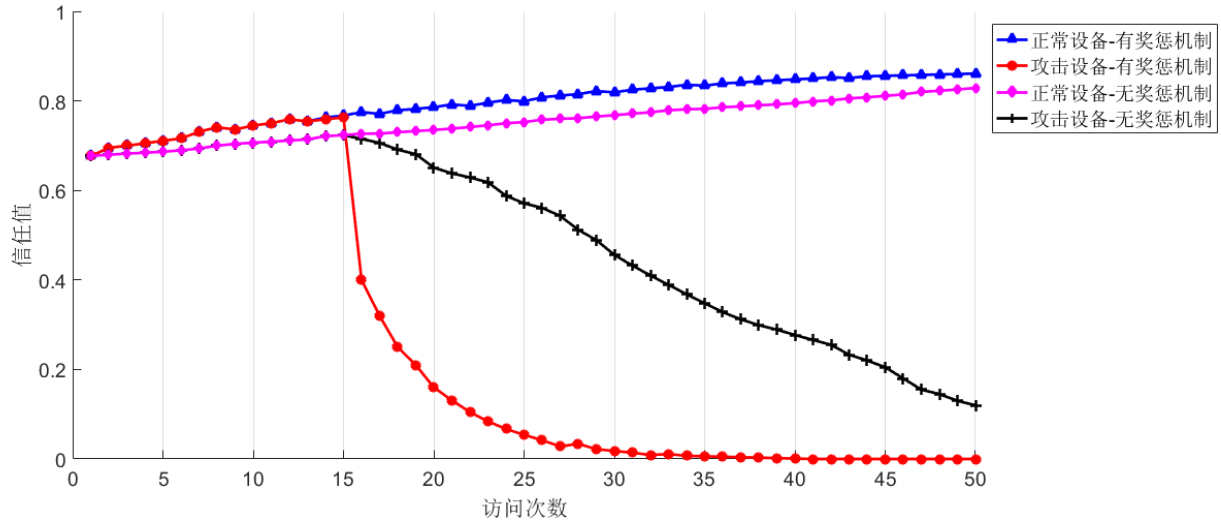

图 5.9 奖惩机制有效性实验结果图

可以观察到使用奖励因子可以使信任值的曲线斜率更大，从而更快地积累信任值。而对于攻击行为设备，惩罚因子可以使信任值呈指数形式下降，极大提高攻击行为拦截率，提高了信任评估算法的灵敏性，能够更快地检测到攻击行为并做出反应。

接下来再从访问主体信任等级角度来验证奖惩机制的有效性，实验结果如图 5.10 所示。

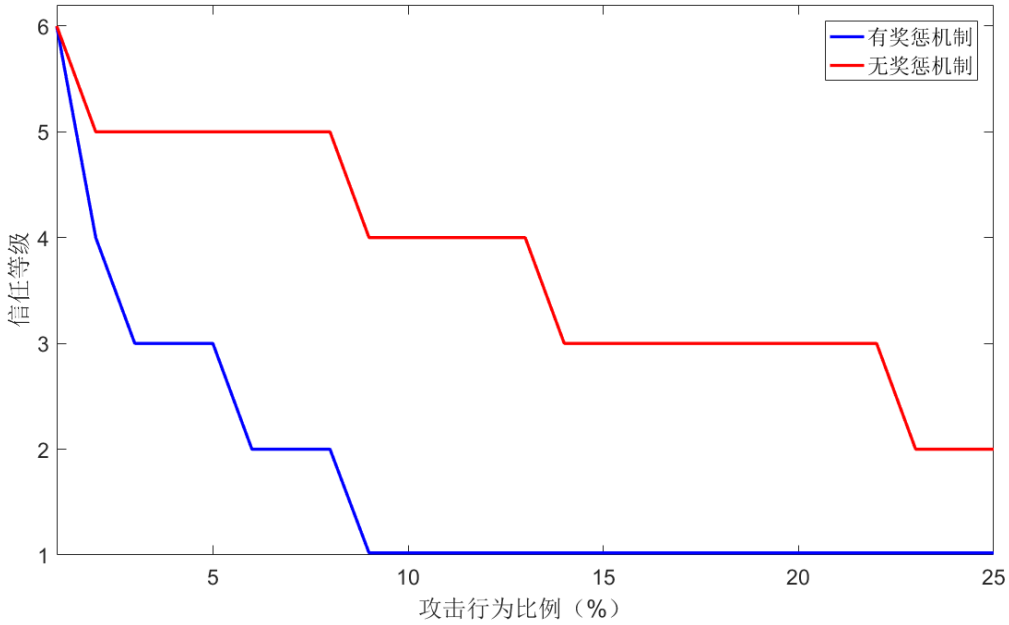

图 5.10 奖惩机制对信任等级变化的影响

攻击行为比例不断增加时，本文提出的信任评估算法能够迅速响应，并大幅降低访问主体的信任等级。当攻击行为比例达到 6%时，该算法已经将信任等级降为不可信等级；当攻击行为比例为 9%时，信任等级已经降至非常不可信等级。相比之下，无奖惩因子情况下信任等级下降速度较慢，在相同攻击行为比例区间内最终信任等级也只降到不可信等级。本文提出的信任评估算法之所以能够更加灵敏地应对攻击行为，得益于引入了 XGBoost-GRU 行为检测模型和攻击行为惩罚机制。行为检测模型负责准确识别攻击行为，惩罚机制负责通过迅速降低信任等级来应对攻击行为，最终实现了快速降低恶意访问主体信任等级的目的。

该实验能够证明本文提出的信任评估算法可以凭借奖惩因子有效防止设备的恶意行为，并且可以根据攻击行为严重程度动态调整惩罚因子，使得访问主体的信任值以不同幅度下降，快速达到非常不可信等级。证明了引入 XGBoost-GRU 行为检测模型对于阻止物联网入侵攻击的有效性，能够比传统信任评估算法更加灵敏地处理存在攻击行为的访问主体。另一方面，奖励因子的存在可以使行为良好的访问主体更容易达到十分可信的信任等级。

实验二：验证本算法能够根据访问主体的区别进行动态计算，能够对于设备和用户针对性做出评估

本实验各选取一个信任等级为非常可信的设备和用户，两者初始信任值相同，历史访问行为也相似。实验中会以相同的幅度降低两个访问主体的硬件行为和网络行为相关行为参数，两者信任值随参数变化结果如图 5.11 所示。

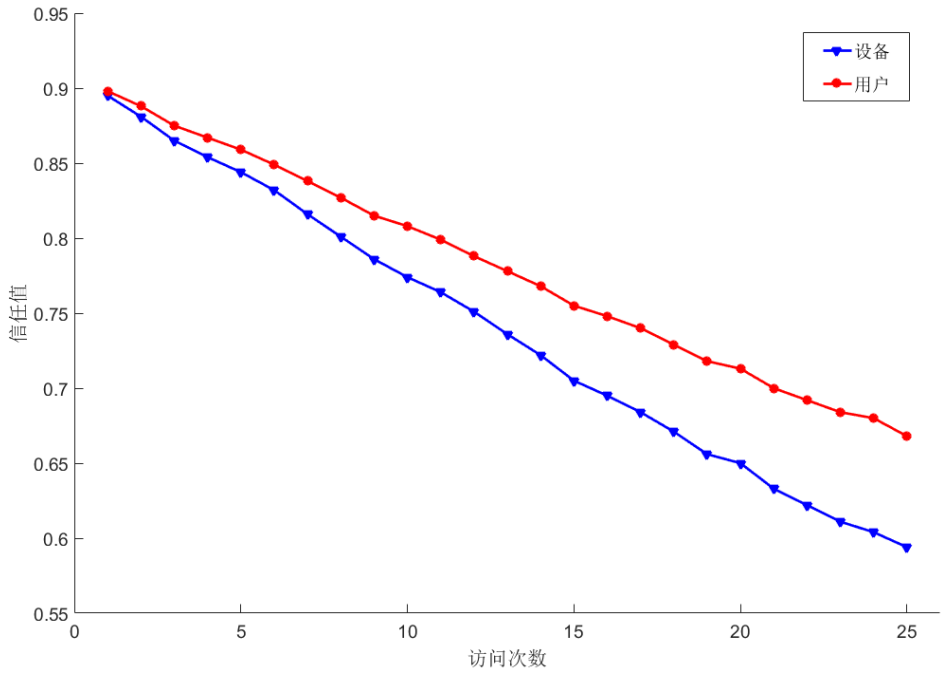

图 5.11 物联网设备/用户信任值变化趋势

从图 5.11 可以看出，设备和用户的初始信任值都在 0.89 左右，信任等级属于非常可信，此时设备和用户的硬件行为参数和网络行为参数数值均相同。随后开始降低这两个行为的行为参数数值，变化幅度相同。相比较而言设备对于硬件行为和网络行为的变化更加敏感，下降幅度比用户更大，且最终的信任值比用户更小。这与物联网设备安全性较差、网络环境相对稳定的特征相符合。当设备安全性和网络环境发送变化时，能够更加迅速的调整设备的信任值，这些属性变化对于用户的信任值影响较小。该实验可以证明本文提出的信任评估算法可以针对物联网环境下不同类型的访问主体的特点做动态修改，具有更好的计算动态性。

实验三：验证时间衰减因子在本文提出算法中的作用，能够提高算法的稳定性和抗攻击性

该实验通过对比相同行为参数的物联网访问主体分别在有时间衰减因子和无时间衰减因子情况下信任值变化趋势，验证时间衰减因子的有效性。图 5.12 展示了有无时间

衰减因子对访问主体信任值变化的影响。

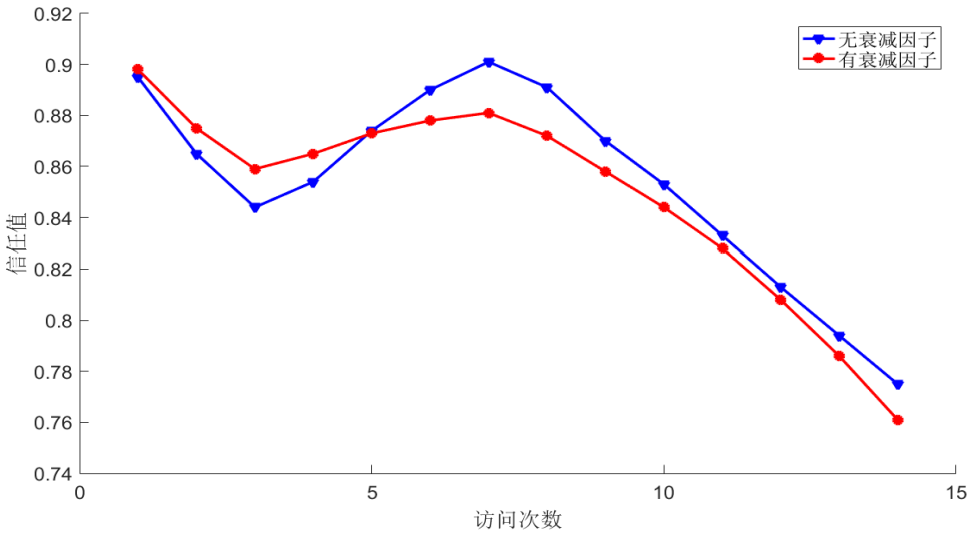

图 5.12 时间衰减因子对信任值影响

两个访问主体的初始信任值为 0.89，并且前五次访问都为越权访问行为，在第 3、7 次访问改变访问的方式，不断在越权访问和正常访问之间切换。通过分析可以得出，本文提出的算法会结合同一访问主体的历史访问行为，使得访问主体的信任值更加稳定。算法在计算历史行为良好的访问主体信任值时会减小信任值下降的幅度，相反的对于历史行为不好的访问主体，时间衰减因子也能够限制其信任值上升的幅度。同时随着恶意行为占历史行为比例的增加，最终信任值会比无奖惩因子的情况低。

下一步为不同时间跨度的历史行为对访问主体信任值的影响的研究，图 5.13 展示的是两个访问主体在不同时间跨度下的行为占比。

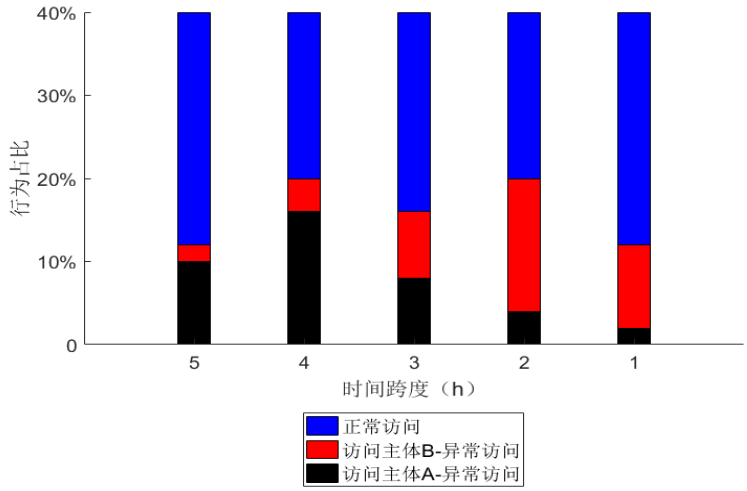

图 5.13 访问主体历史行为占比

可以看出访问主体 A 的异常访问集中在前三个小时，访问主体 B 异常访问集中在后三个小时，随后两个访问主体均开始进行正常访问。访问主体 A、B 在图 5.13 所示的历史行为前提下，后续五次访问的信任值变化趋势如图 5.14 所示。

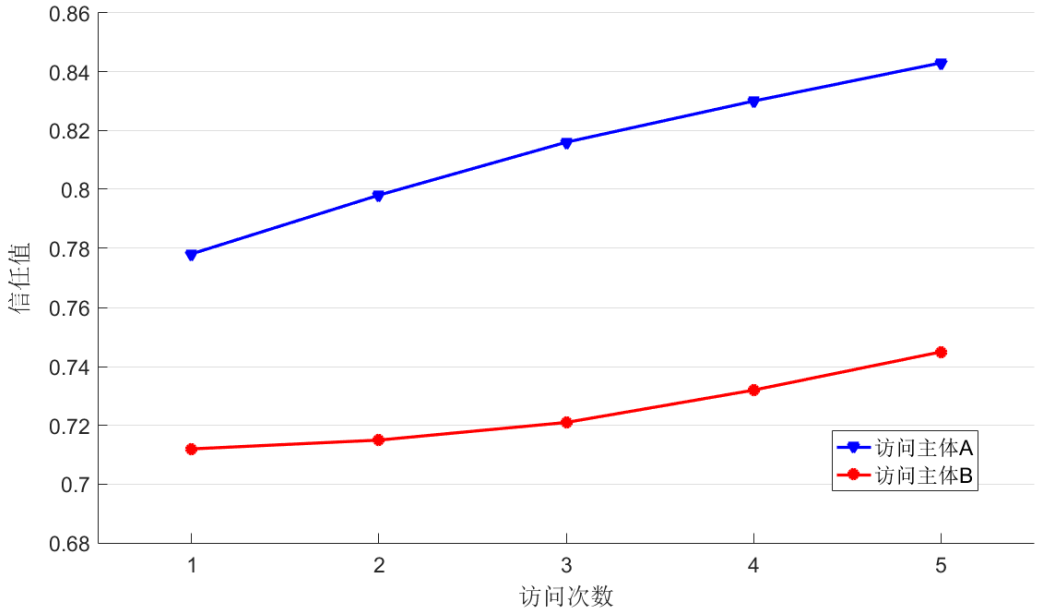

图 5.14 不同历史行为对访问主体信任值的影响

主体 A 的初始信任值比主体 B 高，同时信任值上升幅度也比主体 B 更大，这是由于 B 历史行为中的恶意行为集中在时间跨度较近的时间段，时间跨度越小，衰减因子越大，也就是意味着较近的历史信任值会以更高的权重影响当前信任值。

通过实验可以总结，时间衰减因子不仅能够提高信任评估算法的稳定性，更能够提高抗攻击性。它可以使得访问主体信任值更加稳定，避免由于设备故障或用户误操作等特殊情况导致的信任值骤减而引起权限收回。然而当恶意行为比例不断增加到一定程度时，时间衰减因子可以促使信任算法注重时间跨度较近的历史，从而加速降低恶意访问主体的信任值并限制其信任值积累的速度。

实验四：验证本文提出的访问控制模型具有优秀的访问控制性能

本实验共构造 50 个物联网访问主体，在 24 小时内持续对访问控制系统进行访问，且根据访问主体类别和行为类别分为 10 类。其中入侵设备/用户每 3 小时会进行一次攻击，所有访问主体在 24 小时内访问相关结果如图 5.15、图 5.16 和表 5.6 所示。

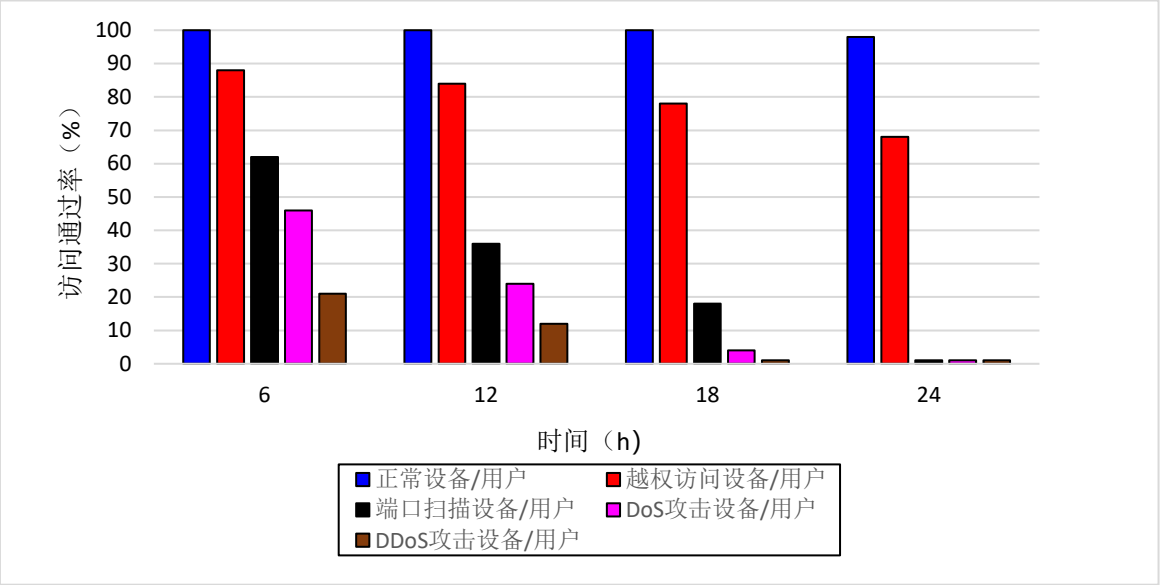

图 5.15 不同行为主体 24 小时访问通过率

图 5.15 展示的是 24 小时内根据行为分类的访问主体每 6 小时内访问通过率，由于入侵行为往往伴随着访问频率的增加，所以使用通过率可以更直观展示访问控制系统效果。可以看出，随着时间的增加，正常设备/用户的访问通过率接近百分之百，越权访问设备/用户的通过率缓慢下降，三类入侵设备/用户的访问通过率以不同的速率快速下降，最终都降为 0。

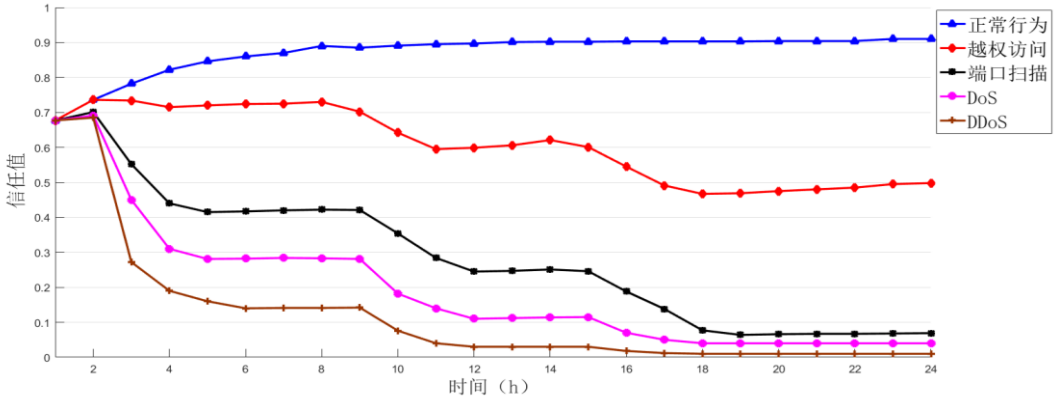

图 5.16 24 小时内不同类别访问主体平均信任值变化趋势

图 5.16 展示的是 24 小时内不同类别访问主体的信任值平均值随时间变化的趋势。正常设备和用户的信任值会随着时间推移逐步上升，其余存在恶意行为的访问主体会在 2h、9h、15h 进行持续三小时的恶意行为。对于越权访问的访问主体，信任值会在越权行为发生期间缓慢下降，恢复正常行为后信任值会逐步回升。另外三种存在入侵行为的

访问主体的信任值会在入侵行为期间迅速下降，同时由于存在惩罚机制，即使后续进行正常访问，信任值也不会突破阈值。且不同种类入侵的信任值下降速度也不相同，入侵等级越高，下降的速度越快。第一次入侵结束后，DDoS 攻击组的设备和用户的信任等级已经降为非常不可信，DoS 攻击组和端口扫描组的设备和用户在第三次入侵结束后信任等级降为非常不可信。

24 小时内访问控制模型对行为的可信判断相关性能参数如表 5.6 所示。

表 5.6 模型访问控制性能参数表

判断类型	不可信行为	可信行为
不可信判断	11535	169
可信判断	26	11984
精度	0.9976	
召回率	0.9856	

从表中数据可以看出，精度和召回率达到 99.76%和 98.56%，说明该 BD-ZTBAC 模型能够实现精准的访问控制功能，能够有效防止物联网恶意设备和用户的入侵行为，证实 XGBoost-GRU 行为检测模型引入的有效性。

总结以上四个实验可以证明，本文提出的信任评估算法，可以将“信任”量化计算出一个具体数值，能够解决信任值计算中模糊、难以量化的问题。在行为参数获取阶段凭借 XGBoost-GRU 模型在攻击行为检测上良好的表现，提高了对异常行为访问主体的捕获，捕获到攻击行为后使用奖惩机制快速响应攻击行为，迅速降低访问主体信任等级，抵御来自外部的入侵。对于来自系统内部的异常行为，通过访问、网络、硬件多角度行为参数，综合计算出信任值，能够有效捕捉内部设备和用户的异常，提高算法的抗攻击性。并且可以根据访问主体的类别调整权重，以应对不同的物联网环境，提高算法的灵活性。此外通过引入时间衰减因子考虑历史信任值的作用，使得信任评估算法更加稳定。而使用该算法的 BD-ZTBAC 模型能够实现对访问的精准控制，有效阻挡攻击行为，并证明该模型适用于物联网接入云计算服务的应用场景。

5.5 本章小结

本章节针对传统访问控制模型在物联网场景下防护性能不足、授权灵活度低等问题，

提出了结合行为检测机制的零信任访问控制模型 BD-ZTBAC。然后从模型相关定义开始，阐述了访问控制流程和信任评估流程，最终将该模型与一些传统访问控制模型进行横向对比，突出该模型的优势。同时阐述了该模型与物联网场景密切相关的原因，以及该模型对物联网场景做出的定制和修改。同时通过四个实验证明 BD-ZTBAC 模型具有稳定性和强抗攻击性，能够适用于物联网环境，证实本文提出的信任评估算法能够根据物联网设备和用户的特点和行为动态评估信任值，符合零信任框架的要求，确保了访问控制模型的可靠性和动态性。

6 总结与展望

6.1 总结

随着信息技术的迅速发展，越来越多的个人和企业选择将服务部署在云端。然而这对于物联网设备和用户接入服务无疑带来了各种安全隐患，如越发多样的入侵方式、突破物理边界的内部攻击、复杂多样的物联网环境，这些因素时刻让云计算服务提供者担忧云计算资源的安全。本文充分研究访问控制技术和入侵检测相关技术的现状并进行了分析。针对物联网接入云计算服务安全问题，本文结合 XGBoost-GRU 行为检测模型、基于访问主体的信任评估算法和零信任架构，设计出面向物联网的零信任访问控制模型。主要研究工作总结如下：

（1）对课题研究涉及的访问控制技术、云计算技术、机器学习算法、零信任架构等相关领域的研究现状进行分析，并结合现有研究中的优点和缺陷。结合零信任架构的“从不信任，持续验证”的理念，从整体框架层面说明零信任系统对于解决现有安全问题的可行性，再将框架拆分为更小的模块，从行为检测模块、信任评估算法两方面对访问控制模型进行优化；

（2）设计并实现了基于 XGBoost 算法和 GRU 神经网络的行为检测模型，通过数据优化、特征选取、参数调优等手段训练出能够准确识别攻击行为的深度学习多分类模型。同时使用该模型的性能指标与其他机器学习模型对比，突出 XGBoost-GRU 模型在物联网攻击行为检测领域的优秀性能；

（3）在 FAHP 算法的基础上创新优化，利用行为检测模块作为信任值计算参数来源，提高行为参数可信度。同时根据物联网设备和用户的行为特点构建行为参数指标，用于访问主体信任值的计算，同时引入时间衰减因子和奖惩机制，实现对访问主体的动态信任值计算，并且针对物联网的访问主体区别，根据设备、用户不同动态分配属性权重，以提高算法的准确性和真实性。最后将该信任评估算法用作零信任访问控制模型的核心信任算法；

（4）提出 BD-ZTBAC 访问控制模型，从组成架构、服务授权流程、信任评估流程等方面进行系统描述。最后通过仿真实验，验证信任评估算法和访问控制模型的性能。实验结果证实该模型在物联网安全接入云计算服务场景的应用具有可行性和有效性，

XGBoost-GRU 行为检测模型与信任评估算法的组合增强了系统的可靠性、动态性和稳定性。该模型不仅可以有效保护云计算资源，同时可以满足物联网复杂环境，适用于不同种类访问主体。

6.2 展望

本文提出的零信任访问控制模型在实现物联网安全接入云计算服务领域取得了一定的成果。但是物联网安全领域仍有许多急需解决的问题，因此该项技术仍存在一些不足和需要改进的地方：

（1）进一步研究影响用户信任评估准确性的用户行为参数，尝试标准化行为参数构建过程。现有的模型在行为参数选取通常是基于经验，并没有一个可量化的标准来评判行为参数选取过程是否合理。因此，信任评估模型属性标准化领域值得继续探讨；

（2）优化访问控制模型。本文内容是研究访问主体的信任评估方法，但是访问客体也可以存在信任这一属性。后续可以在此基础上扩展对云计算服务的信任评估，进一步提高访问控制模型的安全性；

（3）使用无监督学习方法进行行为检测。物联网入侵攻击的种类越加多样，本文选用的数据集不能囊括所有恶意行为，而且现实中并没有那么多可使用的标注数据。无监督学习可以很好地解决这一问题。因此，使用无监督学习来检测访问主体异常行为的方向值得研究。

参考文献

[1] 中国信息通信研究院. 云计算发展白皮书(2021)[R]. 2021-07.

[2] 廖子渊, 陈明志, 邓辉. 基于评价可信度的云计算信任管理模型研究[J]. 信息网络安全, 2016(2):7.

[3] .Kolias C, Kambourakis G , Stavrou A , et al. DDoS in the IoT: Mirai and Other Botnets[J]. Computer, 2017, 50(7): 80-84.

[4] Checkpoint: IoTroop Botnet: the full investigation [EB/OL]. [2018-08-21] https://research.checkpoint.com/-iotroop- botnet-full-investigation.

[5] American Council for Technology-Industry Advisory Council (ACT-IAC). ZeroTrust Cybersecurity CurrentTrends[EB/OL].[2019-04-18]https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf.

[6] Tencent Security. Zero Trust Solution White Paper[EB/OL]. [2022-06-01]. https://cloud.tencent.com/developer/article/1636407.

[7] 刘奇旭, 靳泽, 陈灿华, 等. 物联网访问控制安全性综述[J]. 计算机研究与发展, 2022, 59(10): 2190-2211.

[8] Ouaddah A, Bouij-Pasquier I, Abou Elkalam A, et al. Security analysis and proposal of new access control model in the Internet of Thing[C]//2015 international conference on electrical and information technologies (ICEIT). IEEE, 2015: 30-35.

[9] Servos D, Osborn S L. Current research and open problems in attribute-based access control[J]. ACM Computing Surveys (CSUR), 2017, 49(4): 1-45.

[10] Li J, Yao W, Zhang Y, et al. Flexible and fine-grained attribute-based data storage in cloud computing[J]. IEEE Transactions on Services Computing, 2016, 10(5): 785-796.

[11] Alam Q , Malik S U R , Akhunzada A , et al. A Cross Tenant Access Control (CTAC) Model for Cloud Computing: Formal Specification and Verification[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(6): 1259-1268.

[12] Almutairi A, Sarfraz M I, Ghafoor A. Risk-aware management of virtual resources in access controlled service-oriented cloud datacenters[J]. IEEE Transactions on Cloud Computing, 2015, 6(1): 168-181.

[13] 高艳. 基于行为的云计算访问控制模型研究[D]. 山东师范大学, 2015.

[14] Shen C, Shi L, Zhang H, et al. Trusted Computing and Trusted Cloud Security Framework[J]. Science and Management, 2018, 38(2): 1-6.

[15] Bhatt S, Patwa F, Sandhu R. ABAC with Group Attributes and Attribute Hierarchies Utilizing the Policy Machine[C]// Acm Workshop on Attribute-based Access Control. ACM, 2017: 17-28.

[16] Das S, Sural S, Vaidya J S, et al. Policy Adaptation in Hierarchical Attribute-based Access Control Systems[J]. ACM Transactions on Internet Technology, 2019, 19(3): 1-24.

[17] 谢绒娜, 李晖, 史国振, 等. 基于属性轻量级可重构的访问控制策略[J]. 通信学报, 2020, 41(2): 11.

[18] 陈懋. 基于信任的云计算访问控制系统的设计与实现[J]. 现代电子技术, 2016, 39(11): 4.

[19] 邓三军, 袁凌云, 孙丽梅. 基于信任度的物联网访问控制模型研究[J]. 计算机工程与设计, 2022, 43(11): 7.

[20] 潘瑞杰, 王高才, 黄珩逸. 云计算下基于动态用户信任度的属性访问控制[J]. 计算机科学, 2021.

[21] 张亚萍, 郭银章. 基于信任度与策略相似度的访问策略合成研究[J]. 计算机与数字工程, 2022(003): 50.

[22] 石秀金, 张梦娜. 面向医疗大数据基于零信任的UCON访问控制模型[J]. 智能计算机与应用, 2021, 11(5): 6.

[23] Kindervag J. Build security into your network’s dna: The zero trust network architecture[J]. Forrester Research Inc, 2010, 27.

[24] 潘吴斌, 任国强. 软件定义边界SDP：概念、技术及应用研究综述[J]. 数字通信世界, 2021(03): 192-195.

[25] 朱良海, 张义超, 袁震. 构建基于SDP技术的网络安全体系[J]. 网络安全和信息化, 2019(12): 109-112.

[26] Zscaler.The chalenge with today's network security in a cloud-first world [EB/OL]. [2020-05-31]. htps://www. zscaler.com/products/zscaler-internet-access.

[27] 中国信息通信研究院. 零信任发展洞察报告(2021)[R]. 2021-12.

[28] 马健, 孙鹏. 基于云计算技术的计算机网络安全存储[J]. 电视技术, 2019, 43(20): 18-19.

[29] 龙涛. Task-and-role-based access-control model for computational grid[J]. 重庆大学学报：英文版,

2007, 6(4): 7.

[30] 徐帅. 云环境中数据安全及访问控制模型研究[D]. 华东理工大学, 2014.

[31] Sibai R E, Gemayel N, Abdo J B, et al. A survey on access control mechanisms for cloud computing[J]. Transactions on Emerging Telecommunications Technologies, 2020, 31(2): e3720.

[32] 张立强, 吕建荣, 严飞, 等. 可信云计算研究综述[J]. 郑州大学学报:理学版, 2022, 54(4): 1-11.

[33] 吴云坤, 姜博, 潘瑞萱, 等. 一种基于零信任的SDN网络访问控制方法[J]. 信息网络安全, 2020(8): 10.

[34] 蒋岑. 大数据和云计算在物联网中的应用研究[J]. 软件, 2022, 43(10): 109-112.

[35] Bevish Jinila Y, Prayla Shyry S, Christy A. A Multi-component-Based Zero Trust Model to Mitigate the Threats in Internet of Medical Things[C]//Data Engineering for Smart Systems: Proceedings of SSIC 2021. Springer Singapore, 2022: 605-613.

[36] LI Xin. Access Control Strategy Based on Trust under Cloud Computing Platform[C]//IEEE. 2018 International Conference on Virtual Reality and Intelligent Systems (ICVRIS). New York: IEEE, 2018: 327-330.

[37] Zhao Z, Lei S. Attribute-based Access Control with Dynamic Trust in a Hybrid Cloud Computing Environment[C]// International Conference on Cryptography. ACM, 2017: 112-118.

[38] 刘建生, 游真旭, 乐光学, 等. 网络信任研究进展[J]. 计算机科学, 2018, 45(11): 13-28.

[39] Marsh S P . Formalising Trust as a Computational Concept[J]. Thesis University of Stirling, 1999.

[40] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management[C]//Proceedings 1996 IEEE symposium on security and privacy. IEEE, 1996: 164-173.

[41] 李景仙. E-learning服务的用户信任评估模型及算法研究[D]. 南京航空航天大学. 2012.

[42] Yan Z, Li X, Wang M, et al. Flexible data access control based on trust and reputation in cloud computing[J]. IEEE transactions on cloud Computing, 2015, 5(3): 485-498.

[43] Vanickis R, Jacob P, Dehghanzadeh S, et al. Access control policy enforcement for zero-trust-networking[C]//2018 29th Irish Signals and Systems Conference (ISSC). IEEE, 2018: 1-6.

[44] Rose S, Borchert O, Mitchell S, et al. Zero trust architecture[R]. National Institute of Standards and Technology, 2020.

[45] 田由辉. 基于零信任架构的网络安全防护思路[J]. 信息技术与信息化, 2020(5): 4.

[46] Chen T, Guestrin C. Xgboost: A scalable tree boosting system[C]//Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining. 2016: 785-794.

[47] Verma P, Anwar S, Khan S, et al. Network intrusion detection using clustering and gradient boosting[C]//2018 9th International conference on computing, communication and networking technologies (ICCCNT). IEEE, 2018: 1-7.

[48] 钱程. 基于改进神经网络的入侵检测算法的研究[D]. 河北师范大学, 2020.

[49] Zeeshan M, Riaz Q, Bilal M A, et al. Protocol-based deep intrusion detection for dos and ddos attacks using unsw-nb15 and bot-iot data-sets[J]. IEEE Access, 2021, 10: 2269-2283.

[50] Popoola S I, Adebisi B, Ande R, et al. smote-drnn: A deep learning algorithm for botnet detection in the internet-of-things networks[J]. Sensors, 2021, 21(9): 2985.

[51] Hu C T. Attribute based access control (ABAC) definition and considerations[J]. 2014.

[52] 姚敏, 黄燕君. 模糊决策方法研究[J]. 系统工程理论与实践, 1999, 19(11): 61-64.

[53] Koroniotis N, Moustafa N, Sitnikova E, et al. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset[J]. Future Generation Computer Systems, 2019, 100: 779-796.