文章编号：2095-2163(2021)05-0047-06 中图分类号：TP393.4 文献标志码：A

面向医疗大数据基于零信任的UCON访问控制模型

石秀金，张梦娜
（东华大学 计算机科学与技术学院，上海 201620）

摘 要：医疗大数据的共享在现代医疗技术和服务中发挥着重要作用。针对医疗大数据共享过程中的安全性需求，提出了基于零信任和UCON的医疗大数据访问控制模型ZT-UCON。该模型将零信任思想与支持动态连续访问的UCON模型相结合，利用UCON模型的授权、义务和条件等访问控制策略，构建了面向医疗大数据访问控制决策方案。通过在医疗大数据访问控制的一个典型案例中应用ZT-UCON模型，并对比典型的传统访问控制模型，验证了ZT-UCON的优势。结果表明：基于零信任的UCON访问控制模型，可以降低医疗大数据共享过程中过度访问的可能性，以满足医疗大数据访问控制的安全性需求。

关键词：零信任；UCON；医疗大数据；访问控制

A UCON access control model based on zero trust for medical big data

SHI Xiujin, ZHANG Mengna
(College of Computer Science and Technology, Donghua University, Shanghai 201620, China)

【Abstract】 The sharing of medical big data plays an important role in modern medical technology and services. According to the security requirements in the process of sharing medical big data, a medical big data access control model ZT-UCON based on zero trust and UCON was proposed. The model combines the idea of zero trust with the UCON model, which supports dynamic continuous access, and uses the access control policies of UCON model, such as authorization, obligation and condition, to construct a pre-decision scheme for the access control of medical big data; By applying the ZT-UCON model in a typical case of medical big data access control and comparing with the typical traditional access control model, the advantages of ZT-UCON are verified. The results show that the UCON access control model based on zero trust can reduce the possibility of excessive access issues in the process of sharing medical big data, so as to meet the security requirements of medical big data access control.

【Key words】 zero trust; usage control; big data; access control

0 引 言

随着“互联网+医疗”的快速发展，人们可以通过移动终端便捷获取各类医疗相关资源，网上挂号、在线问诊等功能让人们足不出户便可享受丰富的医疗资源。2018年9月，国家卫健委发布了《国家健康医疗大数据标准、安全和服务管理办法（试行）》[1]，对于医疗大数据的开放共享机制提出了明确的要求。近年来，在医疗数据的产生端和管理端，医疗大数据的快速增长和共享过程中，医疗大数据安全问题如数据的泄露、设备的攻击等时有发生，给患者隐私造成了很大的隐患[2]。传统的仿问控制模型，通常以静态的访问控制策略授予访问权限，已经难以适应于医疗大数据的安全性需求[3]。

随着医疗大数据共享的普遍化，人为因素占据着安全问题的重要部分，支持动态连续的访问控制技术越来越受重视。作为新一代访问控制模型UCON(Usage Control)模型，以模型族$UCON_{ABC}$囊括了传统的访问控制模型功能，并且借助独有的“义务”、“条件”组件为访问控制模型增添了“连续性”和“可变性”特征[4]，将更好地适应于云计算大数据环境下的安全性需求。但UCON的本质是基于主客体属性匹配外，加“义务”执行和“条件”满足来进行访问权限的控制，易出现两种极端情况：一是过度授权，给主体开放职责以外的资源访问权限，安全隐患增多；二是授权不足，当访问策略过于严苛时，会影响主体正常的与职责相关的访问请求执行，使得工作效率降低[5]。针对上述情况，引入零信任中最小权限的设定，外加信任评分引擎，综合决定访问权限授予的思想[6]，将信任值作为主体的重要属性，全程参与访问控制决策过程，动态合理地调控访问权限的授权。因此，结合医疗大数据访问控制的安全性需

基金项目：上海市自然科学基金(19ZR1402000)。

作者简介：石秀金(1976-)，男，博士，副教授，主要研究方向：大数据、隐私保护、移动互联网应用；张梦娜(1995-)，女，硕士研究生，主要研究方向：大数据、访问控制。

收稿日期：2021-01-15

求,将零信任思想与 UCON 模型相结合,设计更加适用于医疗大数据共享的访问控制模型和策略。

1 面向医疗大数据的访问控制分析

1.1 主体关系

传统的访问控制模型主要由 3 个基本元素组成,即主体、客体、权限[7]。对于医疗大数据来说,主体可以划分成生产主体和消费主体。生产主体指的是医疗数据的产生机构,是该数据的所有者,通常医疗数据的共享需要得到生产主体的许可。消费主体是对各类医疗资源发起访问请求的主体,生产主体可以同时是消费主体。随着医疗大数据的共享需求的日益增长,医疗机构除本机构内部的正常访问需求,机构外的消费主体访问需求变得更为广泛。因此,在控制权限的过度授予和授权不足 2 种极端情况发生中,需要满足医疗大数据的适当性共享。

1.2 问题分析

"互联网+医疗"的不断发展,医疗数据服务逐渐从"医疗信息化"向"医联体"、"医共体"方向扩展。医疗大数据的共享为这一过程提供了重要的支撑。大数据背景下,数据共享需求不断加深,医疗大数据资源既需要充分的共享,同时也需要进行强有力的保护。因此,通过有效的医疗大数据访问控制,保障数据安全成为现实的需要。从数据的保密性来看,医疗大数据可以划分为"公开、有条件共享、不予共享"3 类[1]。此时访问控制的作用便是有效执行对"有条件共享"资源的安全性保障。从$UCON_{ABC}$模型族提供的功能来看,面向医疗大数据的授权访问更适宜采用预先决策、预先执行义务以及预先满足条件的授权方式,以及需满足属性值的动态变化,以实现动态连续的访问控制。

传统的医疗数据的有条件共享,通常位于医疗机构内部,采用基于角色的访问控制方式[8]。此方式中的授权行为是静态的,即主体拥有对于某些资源的访问权限后,在未出现安全事故的情况下,通常不做改变,这给医疗数据埋下了安全隐患。对于同时存在医疗机构内外的数据共享情况,传统的访问控制方法更是无法预判在已有的访问策略下,允许的访问请求会造成多大的数据安全威胁,故支持访问主体属性可变,且动态连续的访问控制在医疗大数据的共享需求中显得格外重要。

2 面向医疗大数据的访问控制模型

由上述分析可知,面向医疗大数据的访问控制模型需要具备以下特性:

(1)支持医疗大数据访问主体的属性可变。当访问主体的历史访问行为中,存在恶意行为或者访问主体本次的访问请求风险较大时,模型需支持访问主体标识的改变以及信任值的改变,为后续访问行为的信任评估提供参考。

(2)支持动态且连续的访问控制。对于访问主体提出的访问请求,进行连续的审核,根据信任值的变化,实现连续可变的权限授予。

(3)支持医疗大数据的跨域共享。允许医疗机构外的组织在满足访问控制条件下,访问该机构医疗数据,以进行远程医疗、病症研究等工作。

2.1 UCON 模型的基本原理

使用控制模型(Usage Control,UCON)由 Park 和 Sandhu 通过整合传统访问控制、数字权限管理和信任管理而提出的一个通用模型,被称为下一代访问控制模型[9]。模型总共由 6 个元素组成,3 个基本元素分别是主体、客体和权限;3 个拓展元素分别为授权、义务和条件[10]。UCON 模型整体结构如图 1 所示。

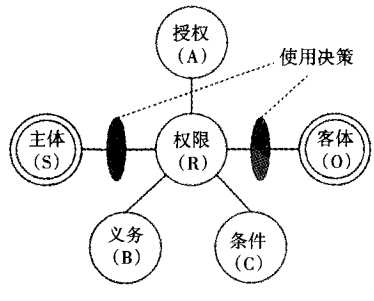

图 1 UCON 模型

Fig. 1 Usage control model

相较于传统的访问控制模型,如自主访问控制模型(Discretionary Access Control,DAC)、强制访问控制模型(Mandatory Access Control,MAC)以及基于角色的访问控制模型(Role-Based Access Control,RBAC)等,UCON 具有连续性和属性可变性两大特性。其中,连续性可通过模型中拓展元素的 *pre* 决策和 *ongoing* 决策方式(其中 *pre* 代表只考虑预定义的决策因素,*ongoing* 代表访问过程中保持访问决策)实现;属性可变性体现在拓展元素执行前后属性的变化状态决定。由连续性和属性可变性的满足情况,可将 UCON 发展成为一个模型族,被称为$UCON_{ABC}$模型族[4]。传统的访问控制模型均可由模型族中的$UCON_{preA_0}$表示,即采用预先授权决策模式,并且不支持属性可变。故当面临具有分布性、社

会性特征的云计算环境时，传统的访问控制便无法提供动态连续的访问控制服务，而基于 UCON 模型研究的访问控制技术则更适用于该访问控制需求。

2.2　面向医疗大数据的访问控制模型构建

2.2.1　基于零信任的 UCON 模型改进

近年来，随着互联网的发展，网络安全事件频频发生，原有的概念“数据中心内部的系统和网络流量是可信的”这一假设是不可取的。零信任网络的概念建立在以下 5 个基本假定之上[11]：

（1）网络环境一直存在着各类威胁因素；

（2）网络环境中的威胁不仅仅来自于外部，甚至内部威胁造成的危害更大；

（3）传统基于 IP 地址的位置信息条件，不足以认定该访问请求的安全；

（4）传统的聚焦于访问主体身份的认证，不足以认定该访问请求安全，即访问主体所使用的设备、所处的真实地理位置等也需作为认证条件；

（5）访问控制策略的评判依据，需根据实际应用场景，详细列举影响因子，设定各影响因子比重，实现个性化、动态化策略制定。

基于零信任的 UCON 模型 ZT-UCON 模型如图 2 所示。ZT-UCON 在原有的 UCON 模型基础上添加了信任评估组件，将原有主体细分为生产主体和消费主题；将原有只和系统有关的条件，拓展为主体条件和全局条件。其中全局条件对应于原有 UCON 模型中的条件。

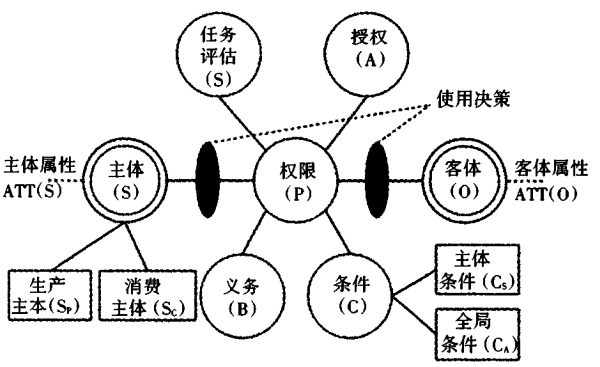

图 2　ZT-UCON 模型

Fig. 2　ZT-UCON model

2.2.2　面向医疗大数据的 ZT-UCON 访问控制决策

ZT-UCON 访问控制决策在连续性方面有预先决策和持续决策。在授权执行访问请求时，属性可变性方面有：属性不可变、执行前属性可变，执行中属性可变，执行后属性可变。

下面从 ZT-UCON 模型的各个组件考虑面向医疗大数据的访问控制决策。

定义：

（1）主体 S 分为生产主体 S_P：医院 A 内部数据拥有者、病患等；消费主体 S_C：医院 A 内外部医护人员、病患、普通大众等；

（2）主体属性 $ATT(S)$：常规属性包括医生的职责、病患所属病种等。可变属性包括主体的信任值。采用执行后可改变方式；

（3）客体 O：各类医疗大数据，其中包括病患个人信息、病患诊疗记录、医学研究数据等；

（4）客体属性 $ATT(O)$：常规属性包括数据病种类别、所属的科室、保密级别等。通常属性不可变；

（5）权限 P：主体 S 对客体 O 的查看、变更和下载操作。如主治医生对病人的病历进行查询、添加诊疗记录操作等；

（6）授权 A：授权规则中划分的权限有两部分来源，一是医疗系统管理员预先制订的访问规则，满足最小权限要求；二是在主体 S 因工作需要主动申请并被管理员批准的权限。采用预先决策方式，不满足授权规则的访问请求，会造成主体当前访问请求信任值的改变，故综合采用 $pre\ A_1$；

（7）义务 B：消费主体 S_C 对各类医疗大数据的访问需完成义务“经由生产主体 S_P 许可”。采用预先决策方式，但不引起主客体属性变化，故综合采用 $pre\ B_0$；

（8）条件 C 包括主体条件 C_S：访问请求时主体的访问地址要求、设备安全要求、访问数据请求量要求等，采用持续决策方式，并且会影响主体当前访问信任值的变化，综合采用 $on\ C_{S1}$；全局条件 C_A：包括系统访问时间、访问并发量等，采用持续决策方式，但不影响主客体属性变化，故综合采用 $on\ C_{A0}$；

（9）信任评估组件 ET：根据信任评估组件对当前主体访问请求行为进行评估，参与访问控制决策过程，评估结果会更新主客体信任值属性，综合采用 $on\ ET_3$。

由上述分析可得，面向医疗大数据的访问控制决策宜采用 $ZT-UCON_{preA_1 preB_0 onC_{S1} onC_{A0} onET_3}$。该模型由 5 个子模型组成，分别为 $ZT-UCON_{preA_1}$、$ZT-UCON_{preB_0}$、$ZT-UCON_{onC_{S1}}$、$ZT-UCON_{onC_{A0}}$ 以及 $ZT-UCON_{onET_3}$，具体可形式化描述为：

（1）$ZT-UCON_{preA_1}$

$-S$、O、$PATT(S)$、$ATT(O)$、$preA$ 分别为主体、客体、权限、主体属性、客体属性，以及预先授权决策；

- $allowed(s,o,p) \Rightarrow preA(ATT(s),ATT(o),p)$；

- $preUpdate(ATT(s))$，$preUpdate(ATT(o))$，可根据实际预授权决策结果更新主客体属性。

(2) $ZT-UCON_{preB_0}$

- S、O、P、$ATT(S)$、$ATT(O)$ 同 $ZT-UCON_{preA_1}$；

- OBS、OBO、OB 分别是义务关联主体、义务关联客体和义务行为；

- $preB$ 为预先义务决策；

- $preOBL \subseteq OBS \times OBO \times OB$ 为预先义务列表；

- $getPreOBL: S \times O \times P \rightarrow 2^{preOBL}$，获取访问请求所需完成的义务列表函数；

- $preFulfilled: OBS \times OBO \times OB \rightarrow \{true, false\}$；

- $preB(s,o,p) = \wedge_{(obs_i,obo_i,ob_i) \in getPreOBL(s,o,p)} preFulfilled(obs_i, obo_i, ob_i)$，当 $getPreOBL(s,o,p) = \emptyset$ 时，即当前访问请求没有对应的义务需要完成，$preB(s,o,p) = true$；

- $allowed(s,o,p) \Rightarrow preB(s,o,p)$。

(3) $ZT-UCON_{onC_{S1}}$

- S、O、P、$ATT(S)$、$ATT(O)$ 同 $ZT-UCON_{preA_1}$；

- T 为时间或事件设置，如 $T = \{always\}$；

- $C_S S$、$C_S O$、C_S 分别是条件关联主体、条件关联客体和主体条件；

- $on\ C_S$ 为持续主体条件决策；

- $on\ CON_S \subseteq C_S S \times C_S O \times C_S$ 为主体条件列表；

- $getOn\ CON_S: S \times O \times P \rightarrow 2^{onCON_S}$，获取访问请求主体所需满足的条件列表函数；

- $on\ Con_S Checked: C_S S \times C_S O \times C_S \times T \rightarrow \{true, false\}$；

- $on\ C_S(s,o,p) = \wedge_{(c_S s_i, c_S o_i, c_{Si}, t_i) \in getOnCON_S(s,o,p)} onChecked(c_S s_i, c_S o_i, c_{Si}, t_i)$，当 $getOn\ CON_S(s,o,p) = \emptyset$ 时，即当前访问请求没有对应的主体条件需要满足，$on\ C_S(s,o,p) = true$；

- $allowed(s,o,p) \Rightarrow true$；

- $stopped(s,o,p) \Leftarrow \neg\ on\ C_S(s,o,p)$；

- $preUpdate(ATT(s))$，$preUpdate(ATT(o))$，可根据实际持续条件决策结果更新主客体属性。

(4) $ZT-UCON_{onC_{A0}}$

- S、O、P、$ATT(S)$、$ATT(O)$ 同 $ZT-UCON_{preA_1}$；

- T 为时间或事件设置，如 $T = \{always\}$；

- $on\ C_A$ 为持续全局条件决策；

- $on\ CON_A$ 为全局条件列表；

- $getOn\ CON_A: S \times O \times P \rightarrow 2^{onCON_A}$，获取访问请求所需满足的全局条件列表函数；

- $on\ Con_A Checked: on\ CON_A \rightarrow \{true, false\}$；

- $on\ C_A(s,o,p) = \wedge_{(onCon_{Ai}) \in getOnCON_A(s,o,p)} on\ Con_A Checked(on\ Con_{Ai})$；

- $allowed(s,o,p) \Rightarrow true$；

- $stopped(s,o,p) \Leftarrow \neg\ on\ C_A(s,o,p)$。

(5) $ZT-UCON_{onET_3}$

- S、O、P、$ATT(S)$、$ATT(O)$、$onET$ 分别为主体、客体、权限、主体属性、客体属性、持续信任评估决策；

- $allowed(s,o,p) \Rightarrow onET(ATT(s),ATT(o),p)$；

- $stopped(s,o,p) \Leftarrow onET(ATT(s),ATT(o),p)$；

- $postUpdate(ATT(s))$，$postUpdate(ATT(o))$，可根据实际持续评估结果更新主客体属性。

(6) $ZT-UCON_{preA_1 preB_0 onC_{S1} onC_{A0} onET_3}$

- $allowed(s,o,p) \Rightarrow preA(ATT(s),ATT(o),p) \wedge preB(s,o,p) \wedge on\ C_S(s,o,p) \wedge on\ C_A(s,o,p) \wedge onET(ATT(s), ATT(o),p)$；

- $stopped(s,o,p) \Leftarrow \neg (preA(ATT(s),ATT(o),p) \vee preB(s,o,p) \vee on\ C_S(s,o,p) \vee on\ C_A(s,o,p) \vee onET(ATT(s),ATT(o),p))$。

3 实例应用与分析

3.1 ZT-UCON 实例应用

本节以具体案例，说明基于 ZT-UCON 的访问请求控制流程。

案例描述：病人 P 之前的诊疗资料存在医院 H1，因工作地点原因，选择到医院 H2 进行术后检查，医院 H2 的医生 D 发起病人 P 的诊疗资料访问请求。

假设条件：医院 H1 与医院 H2 存在资源共享和合作关系。

案例分析：

情况 1 医生 D 所负责的科室和病种与病人 P 相关。当医生 D 申请跨医疗机构访问病人 P 的诊疗信息时，需对该医生进行信任评估，计算医生当前访问行为信任值（信任值的降低值较小或无损耗）和访问历史行为信任值综合计算，并更新其信任值额度。根据评估结果和访问策略决定是否授予权限。

情况 2 医生 D 所负责的科室和病种与病人 P 无关，当医生 D 申请跨医疗机构访问病人 P 的诊疗信息时，对该医生进行信任评估，计算医生当前访问行为信任值（信任值的降低值较大）和访问历史行为信任值综合计算，并更新其信任值。该医生将通

过损耗其信任值额度获取访问权限，会导致其额度减少到零，对该医生后续访问操作进行限制。

访问控制流程图如图 3 所示，具体描述如下：

（1）用户认证阶段：医生 D 使用其账号 $id(D)$ 登录医院系统。如，EMR 系统或 PACS 系统。将病人 P 的就诊 $id(P)$ 输入至系统中，系统认证 $id(D)$ 和 $id(P)$ 是否存在，并对两者属性进行匹配，匹配成功则开放 $id(D)$ 对于 $id(P)$ 的最小权限；

（2）信任评估阶段：$id(D)$ 发起对 $id(P)$ 的电子病历访问申请，根据 $id(D)$ 和 $id(P)$ 之间的属性相关性，对医生 D 的当前访问行为信任值进行计算并将结果保存到历史行为中。若两者属性相匹配或存在关联关系，则信任值不发生损耗或有较小损耗值；若两者相关性较小或无关，则表示医生 D 存在异常访问行为，信任值将有很大的损耗。根据三段滑动窗口分别计算出医生 D 的历史行为信任值，最后得出综合信任值，参与访问控制决策；

（3）访问策略决策阶段：医生 D 针对医院系统 H1 或 H2 发出关于病人 P 的相关诊疗数据 F 时，还需执行一定的义务和满足系统设定的一些条件。如敏感数据访问需要得到病人 P 的署名，医生 D 请求发出时间、地点符合系统要求等，并且义务和条件可根据具体应用场景，确定是否在整个访问控制阶段持续监测，一旦不满足上述设定，则立即终止访问行为。

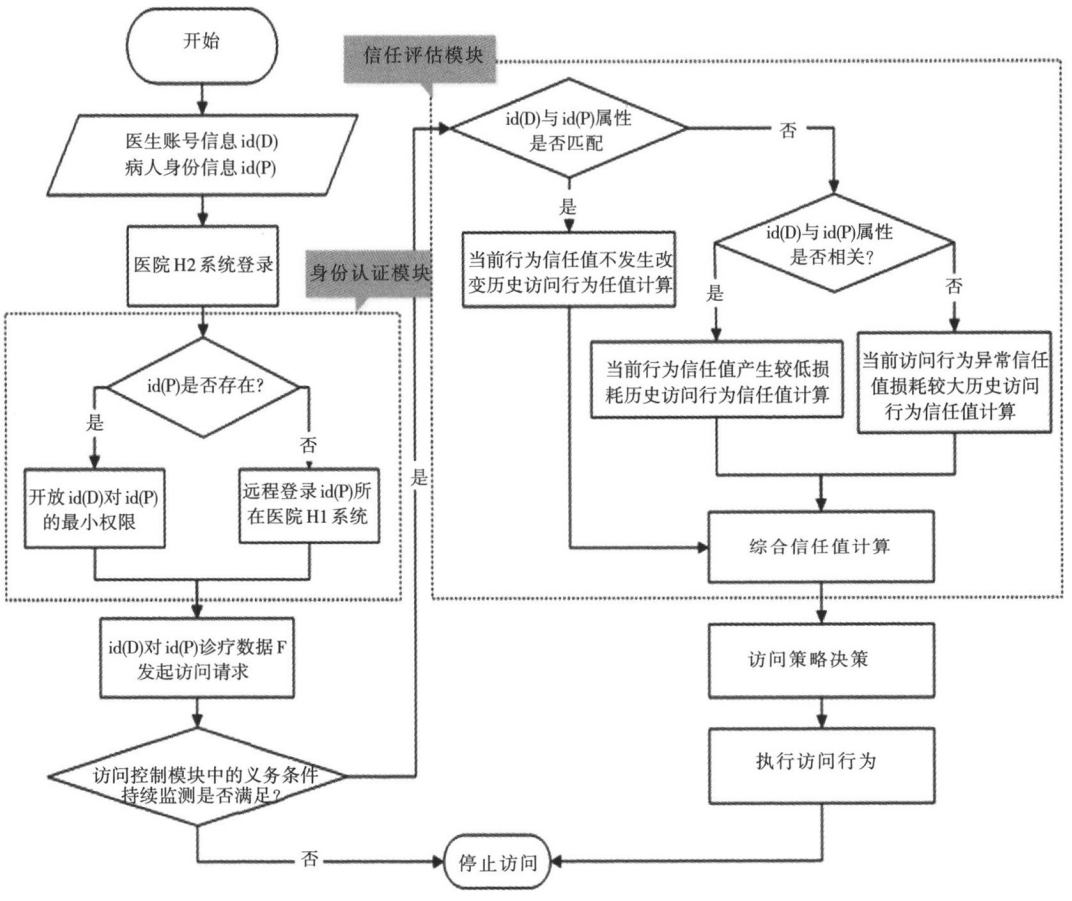

图 3　医疗数据共享访问控制流程图

Fig. 3　Medical data sharing access control flow chart

3.2　ZT-UCON 模型分析

结合 ZT-UCON 模型的访问控制决策，定义和实际应用访问控制流程，将从以下几个方面对 ZT-UCON 的优缺点进行分析。

（1）安全性分析。在传统的访问控制下，通常能保证医疗机构内部数据的安全访问，但随着系统数据类别增多、数据来源广泛，系统数据量快速增长，系统的安全访问需求以及数据共享需求得不到满足。ZT-UCON 模型通过将主体类别划分为生产主体和消费主体，以及将条件类别划分为主体条件和全局条件，提供了更细粒度的访问控制决策，满足医疗大数据背景下的安全性需求。

(2)可用性分析。通常在访问控制中,用户的权限完全由管理员手动分配,已造成权限过度授予问题。在ZT-UCON模型中,管理员只需分配初始最小权限,以满足主体日常工作需求,后续权限的添加由主体根据工作需要提出申请。当主体访问行为出现异常情况时(如主体在一段时间内多次访问与其职责无关的数据),ZT-UCON的信任评估模块将调整其信任值。随着信任值额度的快速消耗,将限制该主体恶意行为。

(3)适用性分析。本文主要解决的是医疗大数据的共享型需求,以及对于医疗大数据主体访问权限过度授权问题,所以对于有数据共享型需求以及过度授权防控需求的领域来说,ZT-UCON可从授权、条件、义务决策过程方面进行按需调整,故同样适用于上述领域。

4 结束语

基于零信任思想和UCON模型的连续性决策以及属性可变特征所提出的ZT-UCON模型,将信任评估模块添加到访问控制决策中,并对主体行为进行持续性评估,动态更新主体信任值属性,更好地满足了医疗大数据所面临的动态多变的云环境安全访问控制需求。后续将进一步深入研究信任评估过程,在满足持续评估功能的基础上,进一步提高信任值评估过程中的计算效率。

参考文献

[1] 国家卫健委印发国家健康医疗大数据标准、安全和服务管理办法(试行)[J]. 中国医药生物技术,2018,13(5):431.
[2] 朱卫红. 医疗信息的隐私保护研究[D]. 杭州:中国计量大学,2016.
[3] 施明月. 基于风险访问控制的医疗大数据安全与隐私保护模型研究[D]. 昆明: 云南财经大学,2020.
[4] Jaehong Park, Ravi Sandhu. The $UCON_{ABC}$ usage control model [J]. ACM Trans Inf Syst Secur:2004,7(1):128-174.
[5] Ma K, Yang G, Xiang Y. RCBAC: A risk-aware content-based access control model for large-scale text data [J]. Journal of Network and Computer Applications, 2020, 167:102733.
[6] 左英男. 零信任架构在关键信息基础设施安全保护中的应用研究[J]. 保密科学技术,2019 (11):33-38.
[7] 李敏,于仕. 基于UCON改进模型在云环境虚拟访问控制中的应用[J]. 科学技术与工程,2018,18(21):82-87.
[8] 卢宁. 基于信任和风险自适应的医疗大数据访问控制模型研究[D]. 昆明:云南财经大学,2019.
[9] Jaehong Park,Ravi Sandhu. Usage control:a unified framework for next generation access control [D]. George Mason University, 2003.
[10] Xinwen Zhang, Francesco Parisi-Presicce, Ravi Sandhu, Jaehong Park. Formal model and policy specification of usage control [J]. ACM Transactions on Information and System Security (TISSEC), 2005,8(4):351-387.
[11] 荣钰,催应杰,任亮,杨庆华. 零信任安全模型在云计算环境中的应用研究[A]. 中国计算机学会.第32次全国计算机安全学术交流会论文集[C]//中国计算机学会:中国计算机学会计算机安全专业委员会,2017:5.

(上接第46页)

制系统设计方法。构建自导飞行装置的控制参数采集模型,根据自导飞行装置的飞行特点,进行自导飞行装置末端姿态偏移的空间规划,建立自导飞行装置的运动学方程,采用惯导误差反馈和自适应补偿方法,构建自导飞行装置控制系统的控制律,实现控制系统的优化设计。研究得知,本文设计的自导飞行装置控制的稳定性较好,误差较低。

参考文献

[1] 马思迁, 董朝阳, 马鸣宇, 等. 基于自适应通信拓扑四旋翼无人机编队重构控制[J]. 北京航空航天大学学报, 2018, 44(4): 841-850.
[2] FORNI F, SEPULCHRE R. A differential Lyapunov framework for contraction analysis [J]. IEEE Transactions on Automatic Control, 2013, 59(3):614-628.
[3] 张国山, 郝婧漩. 基于位置修正机制和模型更新策略的跟踪算法[J]. 信息与控制, 2020, 49(2): 177-187.
[4] 张海南, 游晓明, 刘升. 动态进化与交互学习机制融合的蚁群算法[J]. 信息与控制, 2020, 49(3): 297-305.
[5] 苏耀伦, 施惠元, 苏成利,等. 基于DOB的多变量非最小状态空间预测控制[J]. 信息与控制, 2020, 49(3): 356-364.
[6] 魏新江, 张林青. 一类随机系统基于干扰观测器的抗干扰控制[J]. 控制与决策, 2017, 32(5):939-942.
[7] SHI H Y, SU C L, CAO J T, et al. Nonlinear adaptive predictive functional control based on the Takagi-Sugeno model for average cracking outlet temperature of the ethylene cracking furnace [J]. Industrial Engineering Chemistry Research, 2015, 54(6):1849-1860.
[8] 杨超, 高哲, 黄晓敏,等. 含有有色噪声的非线性分数阶系统自适应扩展卡尔曼滤波器[J]. 信息与控制, 2019, 48(5): 580-588.
[9] 马璐, 刘成菊, 林立民, 等. 基于AM-RPPO的双足机器人适应性行走控制算法[J]. 机器人, 2019, 41(6): 731-741.
[10] 王贵程,吴国新,左云波,等.基于改进蚁群算法包装机器人轨迹规划研究[J].电子测量与仪器学报,2019,33(8):94-100.