南京邮电大学学术型硕士研究生学位论文开题报告

学号	1018041209	姓名	吴嘉余	手机	18761869780
专业	计算机软件与理论	所在学院	计算机学院	导师	柯昌博
已获得的课程学分	30		是否达到培养计划要求	是	
未完成的课程及预计完成时间	无				
补修课程及成绩	无				
初定论文题目	基于风险评估的雾计算访问控制策略动态演化方法研究				
论文选题来源	国家自然科学基金青年项目(Grant 61602262) 江苏省自然科学基金青年项目(Grant BK20150865)				
论文类型	□基础研究 ■应用研究 □综合研究 □其他				

导师对所选课题的基本要求

1、结合自己的专业培养方向，在文献调研的基础上确定论文选题，参考文献不少于 20 篇；

2、论文选题要求具有一定的理论性，争取与实际应用相结合；

3、选题研究目标要明确，研究内容要具体，主要工作及可能的创新要求至少有 2 个方面；

4、论文研究的技术路线（方案)要细化，技术实现要有可行性。

5、明确研究成果，要求结合论文研究发表论文或申请专利。

1. 本报告 A4 纸双面打印，研究生院、学院各一份，导师、学生自留底稿。

一、选题依据(综述报告)

(与选题有关的国内外研究综述，阐述研究目的和实际意义，列出主要阅读参考文献，不少于 20 篇)

1. 国内外研究综述

云计算由于其高性能、低成本、可扩展性等优势得到广泛应用，雾计算作为云计算的扩展，可在终端用户与云计算之间提供计算、 存储及网络服务，可解决云计算的多种弊端,如时延不确定、缺乏移动支持、位置敏感等[1]。雾计算由大量雾节点构成，每个终端设备（用户）连接一个雾节点，雾节点可对收集的数据进行初步分析及临时存储，因此能够降低时延，支持实时分析，解决敏感应用的计算需求。云计算提供更智能化的分析及长久或永久存储[2]。在雾计算中，数据脱离所有者的控制范围,保存在并不完全可信的雾节点中，因此针对数据的访问控制是保证雾计算安全的重要技术。由于雾计算尚处于发展初期，目前关于雾计算隐私保护与访问控制的研究较少，而同样的问题在云计算中得到广泛的研究[6]。

基于风险的访问控制方法是根据用户的风险值来决定当前请求是否允许，访问资源时灵活高效，传统的软件模型使用严格的静态访问控制策略，因此它不能很好地适应动态和异构的环境。Cheng 等[7][3]人提出基于模糊推论的多种用户安全等级访问控制系统，该模型将信息的价值和信息非法暴露的可能性作为一个函数来量化访问的风险，它是基于当前用户的请求、风险的容忍态度和环境动态地控制数据的处理。Ni 等[8][4]人根据模糊推论提出基于风险的访问控制系统，它根据事先定义好的规则来评估访问的风险，满足 Bell-LaPadula(BLP)[9]模型简单的安全性质，这些规则将资源和用户的安全等级作为前因，风险作为结果来构建此系统。这些工作只考虑风险的实体因素，例如用户和资源来量化风险，并没有考虑用户信誉值和用户行为。

Offifice[10][5]提出风险自适应访问控制模型(RAdAC)，主要用于军事方面的使用，它是基于安全和需求来计算并决策是否允许用户访问，此访问控制系统只能应用在军事相关的领域。Britton 等[11]人根据 27 种风险因素并分为 6 组，提出 RAdAC 模型的量化方法，然后针对分组及因素利用事前分配权重来计算风险值。McGraw[12]也同样在 RAdAC 的基础上提出新的模型，该模型先计算当前访问的风险值，然后与访问控制策略(包括风险相关策略和风险无关策略)进行比较，满足则访问被允许。Molloy 等[13]人基于风险等级和访问行为，提出如何量化读访问风险的方法。Shaikh 等[14]人根据用户与资源去评估信任值与风险值的关系，记录用户访问特定资源的历史行为，当信任值大于风险值时，访问被允许。这些工作只考虑用户信誉值来量化风险，但不是面向用户行为。

Djemame 等[15]人以基础设施提供者的视角，提出量化风险的方法。dos Santos 等[16][17][18]人通过设置上下文、数据属性(保密性，完整性和可用性)和历史行为的权重来量化风险。Fall[19][20]等人基于模糊推论，对资源敏感度和用户安全等级来量化风险。Sharma 等[21]人面向健康医疗领域，用户访问行为对请求资源完整性、可用性和保密性的影响，评估行为发生的可能性和历史风险分数等去量化风险。这些工作仅考虑用户信誉值和行为来量化风险，但是没有考虑用户行为产生的结果对风险值的影响。

综上所述，目前关于雾计算隐私保护与访问控制的研究较少，基于风险评估的访问控制方法只考虑用户的实体因素，没有考虑用户信誉值和行为，因此本课题面向雾计算提出基于风险评估的访问控制方法，风险评估考虑用户实体因素、用户信誉值、用户行为和上下文等多个方面。

2. 研究目的

传统的访问控制,例如基于角色的访问控制(RBAC)和多重安全等级的访问控制(Bell-LaPadula)是严格的并且需要确定每一个请求者的安全等级，需要手动控制且耗时多。此外，这些传统的模型没有在访问控制方法中考虑不确定性和风险，这导致不能自适应环境动态地调整策略，例如医疗、紧急情况和军

事等。基于这些不足，我们提出基于风险评估的雾计算访问控制方法。

利用形式化方法定义访问控制模型和执行机制，包括事先定义好的策略和上下文信息，例如运作风险，用户需求和行为的收益等，并且可以利用形式化模型对每个请求做动态分析。此模型可以使用一个函数来表示。公式如下：

$$canAccess(s,o,a,c)=\begin{cases}1, risk(s,o,a,c)<riskThreshold\\ 0, otherwise\end{cases} \quad (1)$$

其中 s 表示用户，o 表示资源，a 是用户访问行为，c 是上下文信息。s,o,a 和 c 作为风险评估函数的输入，风险值作为输出。如果量化的访问风险低于风险阈值，此次访问就被允许。此外，在每次作出判断后访问控制模型将利用审计、责任服务(Obligation Service)或者信誉值系统监控用户的访问行为。

传统的访问控制模型利用可扩展访问控制标志语言(XACML)进行描述，支持策略的执行、访问的请求和响应。该语言由策略管理节点(PAP)、策略信息节点(PIP)、策略决定节点(PDP)和策略执行节点(PEP)组成。PAP 和 PIP 分别可以提供 PDP 风险无关策略和用户或资源的信息，PEP 负责接收请求，PDP 根据访问控制策略作出访问决定。为了满足模型对用户的风险评估，本课题拟对 XACML 策略进行扩展，每个策略包括资源、资源拥有者、量化函数、风险集合函数和风险阈值等元素。

综上所述，主要有三个研究目的：

(1)本课题研究基于风险评估的雾计算访问控制方法，对 XACML 组件进行扩展，加入风险评估框架，并对 XACML 执行引擎进行扩展，使其满足执行需求。

(2)风险评估框架不仅只考虑请求的实体(用户或者资源)，还需考虑用户的访问记录、访问行为和上下文信息。

(3)基于 XACML 策略研究一种支持风险评估的安全策略，如果满足访问控制策略(风险无关策略和风险相关策略)，用户请求将被允许。

3. 实际意义

物联网、网格、云和雾具有分布式、自动重构和动态性的特点，传统的访问控制模型很难满足系统对安全的需求，有以下三个主要的不足：

(1)传统的访问控制策略通常是静态并且严格，因此不能处理异常情况，例如策略需要重写但不能停止系统。

(2)传统的访问控制模型不能满足动态信息安全的需求，在协同环境中很难实现信息共享。

(3)传统的访问控制模型无法处理用户不断改变的访问行为。

策略的不完整或不一致会导致许多异常情况，在医疗和军事环境中策略的重写有两个案例，例如医生或士兵为了挽救病人的生命或完成任务，必须获得限权信息。本课题基于 XACML 策略，支持风险评估，可以使用户得到限权信息，并保证在不停止系统的情况下重写策略，实现策略的自适应。

在提出的访问控制方法中，将风险值表示为 risk(s,o,a,c),它代表在某环境中用户以某种行为访问某种资源的风险值。如果风险值低于风险阈值，请求将被允许。该模型考虑风险因素并根据环境动态的执行请求。

综上所述，本课题有三个实际的意义：

(1)研究基于风险评估的雾计算访问控制方法,对 XACML 组件进行扩展，加入风险评估框架，为预类

攻击和新型计算系统提供自适应的访问控制方法，防止隐私数据的暴露。

(2)在现有的访问控制方法中，不仅考虑用户和资源等实体信息，并且考虑用户访问行为、历史记录和上下文信息，使风险量化更精确并保证每次访问的高效处理。

(3)基于风险的访问控制方法可以在异常情况下保证访问控制策略(风险无关策略和风险相关策略)的正确执行，随时根据环境动态改变策略，使策略更好地适应真实场景。

参考文献

[1]曹咪,徐雷,陶冶.雾计算认证与隐私保护研究综述[J].信息通信技术,2018,12(06):25-33.

[2]汪金苗,王国威,王梅,朱瑞瑾.面向雾计算的隐私保护与访问控制方法[J].信息网络安全,2019(09):41-45.

[3]刘逸敏,周浩峰,王智慧,汪卫.Purpose 融合:基于风险 purpose 的隐私查询访问控制[J].计算机学报,2010,33(08):1339-1348.

[4]唐卓,赵林,李肯立,李瑞轩.一种基于风险的多域互操作动态访问控制模型[J].计算机研究与发展,2009,46(06):948-955.

[5]房梁, 殷丽华, 郭云川,等. 基于属性的访问控制关键技术研究综述[J]. 计算机学报, 2017, 40(7):1680-1698.

[6]Fog computing and its role in the internet of things. In: workshop on Mobile cloud computing. ACM (2012)

[7]P. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner, and A. S. Reninger, “Fuzzy Multi-level Security: An Experiment on Quantifified Risk Adaptive Access Control”, IEEE Symposium on Security and Privacy, pp. 222-230, 2007.

[8]Q. Ni, E. Bertino, and J. Lobo, “Risk-based Access Control Systems Built on Fuzzy Inferences”, ACM CCS, pp. 250-260, 2010.

[9]D. E. Bell and L. J. LaPadula, “Secure Computer Systems: Mathematical Foundations”, Tech. Rep. MTR-2547, vol. 1, 1973.

[10]J. P. Offifice, “HORIZONTAL INTEGRATION: Broader Access Models for Realizing Information Dominance” MITRE Corporation, Technical Report JSR-04-132, 2004.

[11]D. W. Britton and I. A. Brown, “A Security Risk Measurement for the RAdAC Model”, DTIC Document, Tech. Rep., 2007.

[12]McGraw R. Risk-adaptable access control RADAC. In: Privilege (Access) management workshop. NISTeNational Institute of Standards and TechnologyeInformation Technology Laboratory; 2009.

[13]I. Molloy, L. Dickens, C. Morisset, P.-C. Cheng, J. Lobo, and A. Russo, “Riskbased Security Decisions Under Uncertainty”, ACM CODASPY, pp. 157-168, 2012.

[14]R. A. Shaikh, K. Adi, and L. Logrippo, Dynamic Risk-based Decision Methods for Access Control Systems”, Computers & Security (Elsevier), vol. 31, no. 4, pp. 447-464, 2012.

[15]K. Djemame, D. Armstrong, J. Guitart, and M. Macias, “A Risk Assessment Framework for Cloud Computing”, IEEE Transactions on Cloud Computing, vol. 4, no. 3, pp. 265-278, 2016.

[16]D. R. dos Santos, R. Marinho, G. R. Schmitt, C. M. Westphall, and C. B. Westphall, “A Framework and Risk Assessment Approaches for Risk-based Access Control in the Cloud”, Journal of Network and Computer Applications (Elsevier), vol. 74, pp. 86-97, 2016.

[17]D. R. dos Santos, C. M. Westphall, and C. B. Westphall, “Risk-based Dynamic Access Control for a Highly

Scalable Cloud Federation", International Conference on Emerging Security Information Systems and Technologies, pp. 8-13, 2013.
[18]D. R. dos Santos, C. M. Westphall, and C. B. Westphall, "A Dynamic Risk-based Access Control Architecture for Cloud Computing", IEEE NOMS, pp. 1-9, 2014.
[19]D. Fall, T. Okuda, Y. Kadobayashi, and S. Yamaguchi, "Risk Adaptive Authorization Mechanism (RAdAM) for Cloud Computing", Journal of Information Processing, vol. 24, no. 2, pp. 371-380, 2016.
[20]P. Arias-Cabarcos, F. Almenarez-Mendoza, A. Mar ´ ´ın-Lopez, D. D ´ ´ıaz-Sanchez, and ´ R. Sanchez-Guerrero, "A Metric-based Approach to Assess Risk for On Cloud ´ Federated Identity Management", Journal of Network and Systems Management (Springer), vol. 20, no. 4, pp. 513-533, 2012.
[21]M. Sharma, Y. Bai, S. Chung, and L. Dai, "Using Risk in Access Control for Cloud-Assisted eHealth", IEEE HPCC-ICESS, pp. 1047-1052, 2012.

二、选题的研究目标、研究内容、所要解决的主要问题及可能的创新点

1. 研究目标

本课题基于风险评估的访问控制方法，对 XACML 组件进行扩展，加入风险评估框架，它是轻量级的并满足实时的协同访问，通过建立不确定模型，利用软件安全机制来阻止内部攻击，通过改变模型参数适应整个协同平台，其研究目标如下：

(1)对 XACML 组件进行扩展，加入风险评估框架，使其量化用户请求的风险，并对 XACML 执行引擎进行扩展，使其满足扩展后的 XACML 的执行需求；

(2)研究风险评估框架的各个模块，在信誉值模块中分配请求者安全等级的权重，即不确定性函数模型，并在 AIC 模块中分配资源敏感度的权重，即效用性函数模型，将预期威胁分为请求者的访问威胁和请求者访问行为对资源的威胁两部分，最后根据权重线性回归函数和预期理论函数将预期威胁转化为风险值；

(3)在 XACML 策略的基础上提出风险策略，如果满足访问控制策略(风险相关策略和风险无关策略)，请求将被允许，访问控制策略还会根据风险值的变化自适应地调整；

(4)根据前期研究的理论成果，仿真分析并评价风险评估框架，实现 XACML 执行引擎并开发原型系统。

2. 研究内容

基于风险评估的访问控制方法是在雾环境中保证系统安全的主要途径，在访问的过程中，如何量化预期威胁，预期威胁如何转化成风险值；在量化风险值后，如何根据风险策略作出决定，如何根据风险值自适应改变访问控制策略，基于以上问题，本课题主要的研究内容为：

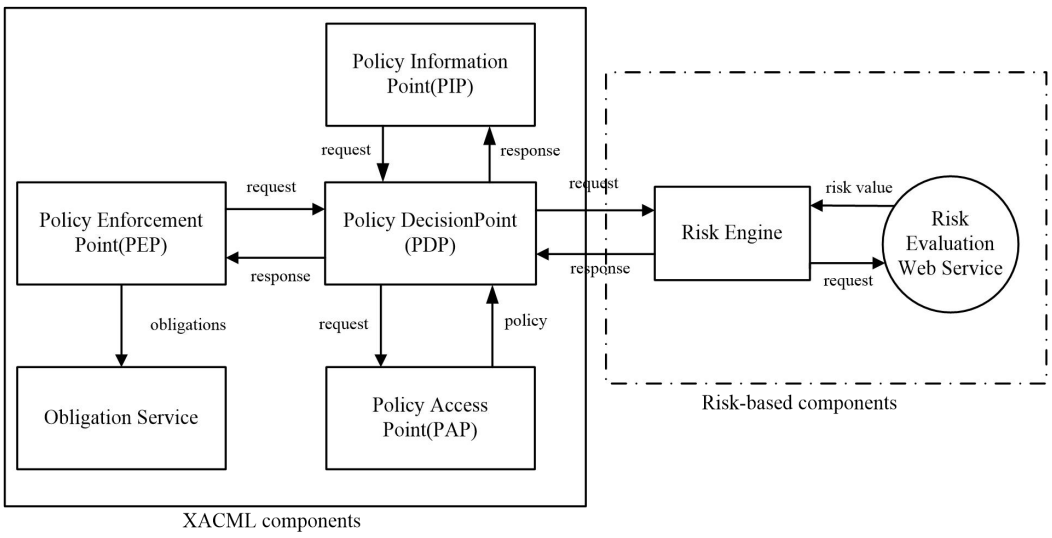

图. 1：基于风险评估的访问控制方法

首先，策略执行节点(PEP)接收用户的访问请求并把请求转发给策略决定节点(PDP),策略信息节点(PIP)将用户和资源的信息提交给 PDP，同时策略访问节点(PAP)根据 PIP 中的信息生成风险无关策略提交给 PDP。然后，PDP 请求风险引擎调用风险评估网络服务量化请求的风险值，并且风险引擎根据量化函数、集合函数、风险值和风险阈值生成风险相关策略提交给 PDP。最后，如果满足访问控制策略(风险无关策略和风险相关策略)，请求将被允许。PDP 将该请求决定提交给 PEP，PEP 判断是否执行用户请求。用户每次访问后，PEP 将用户历史记录反馈给责任服务(Obligation Service)。

(1)面向风险量化的 XACML 组件扩展方法

首先，面向风险量化的需求，研究对 XACML 组件加入风险评估框架的方法，以及对组件扩展后的合理性和正确性进行验证的方法(图 1 虚线部分表示如何在 XACML 的基础上加入风险评估框架)；

其次，为使扩展后的 XACML 组件可以执行，研究 XACML 执行引擎的扩展方法(图 1 实线框中的 Obligation Service 表示 XACML 执行引擎的扩展)；

再次，根据图 1 的访问控制方法，具体研究风险评估框架,通过网络服务量化每次请求的风险值并返回给 PDP，图 2 表示风险评估框架中的三个主要模块；

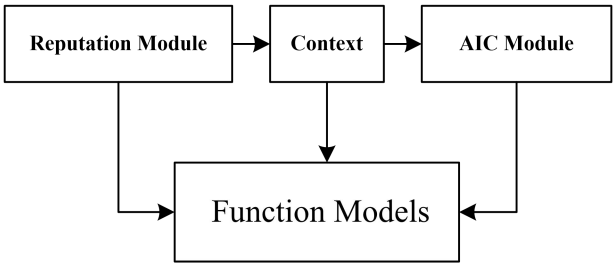

图.2：风险评估框架的三个模块

(2)研究量化预期威胁并将预期威胁转化为风险值的方法

首先,根据用户的历史访问记录研究用户信誉值函数,再根据用户信誉值分配用户安全等级的权重，即不确定性函数，并分析用户访问的预期威胁与上下文的关系。

其次，根据用户访问行为表构建结果代价模型，再基于结果代价建立行为代价模型，然后根据行为代价分配资源敏感度的权重，即效用性函数，并分析用户行为对资源的预期威胁与上下文的关系；

再次，根据权重线性回归和预期理论构建连接函数将预期威胁转化为风险值。

(3)研究风险策略的形式化方法

首先，研究基于 XACML 策略的风险策略，如果满足访问控制策略(风险相关策略和风险无关策略)，用户请求将被允许；

其次，根据风险值研究动态调整访问控制策略的方法。

(4)研究风险评估框架的实验方案并开发原型系统

为验证本课题所提理论方法的可行性与实用性，开发风险评估框架并验证其正确性，并实现基于 XACML 的风险策略，实现基于风险评估的雾计算访问控制方法的原型系统，设计实验并对实验数据进行对比分析。

3. 解决的主要问题

(1)如何使扩展后的 XACML 量化用户请求的风险

首先，如何对 XACML 组件进行扩展，加入风险评估框架，使其支持量化用户请求的风险；其次，如何对 XACML 执行引擎进行扩展，使其满足扩展后的 XACML 的执行需求；再次，怎么保证扩展后的 XACML 的可行性和正确性；

(2)如何分析和量化预期威胁并转化成风险值,使其实现 XACML 执行过程中满足风险量化的需求

首先，如何量化用户访问的预期威胁；其次，如何量化用户行为对资源的预期威胁；再次，如何将预期威胁转化为风险值。

(3)如何形式化风险策略

首先，如何根据现有的 XACML 策略进行扩展，在其基础上加入风险策略；其次，如何根据风险值动态调整访问控制策略。

4. 可能的创新点

与现有的工作相比，本课题主要面向雾计算，提出基于风险评估的访问控制方法，量化每次请求的风险，对用户隐私数据进行保护。而原有的访问控制方法多数是基于角色或多重安全等级，很难满足动态的雾计算环境，此课题可能的创新点为：

(1)风险评估不仅考虑用户信誉值，还考虑用户行为，面向数据完整性、可用性和保密性构建结果代价和行为代价函数来量化风险。

(2)基于 XACML 策略进行扩展，生成完整的访问控制策略(风险无关策略和风险相关策略)。

(3)根据用户风险值的变化自适应调整用户的访问控制策略(风险无关策略和风险相关策略)。

三、研究方法(预期思路或技术路线)及可行性分析

1、 研究方法

(1)对 XACML 进行扩展，加入风险评估框架，使其量化用户请求的风险(图 2)

①增加信誉值模块，用以量化用户访问的预期威胁；②增加 AIC 模块，用以量化用户行为对资源的预期威胁；③增加上下文模块，用以在访问过程中动态改变预期威胁。

对 XACML 执行引擎进行扩展，使其满足扩展后的 XACML 的执行需求(图 1)

①增加责任服务，将用户的访问历史记录传给 XACML 执行引擎的 PDP；②增加风险策略，该策略约束风险评估框架。

(2)量化预期威胁并转化成风险值

①在信誉值模块中量化用户访问的威胁，伪代码图 3 所示：

```
Input:bad,good      //恶意访问次数和友好访问次数
Output:subjectThreat     //用户访问的预期威胁
Initialize:bad←0,good←0,subjectThreat←0,subjectSecurityLevel←0.8;  //初始化
reputationValue←reputationValueFunction(bad,good);  //信誉值函数模型
uncertainty←uncertaintyFunction(reputationValue);  //用户安全等级的权重及不确定性函数模型
subjectThreat←subjectSecurityLevel*uncertainty;  //权重线性回归计算用户访问的预期威胁
end
Return:subjectThreat;
```

图.3:信誉值模块伪代码

②在 AIC 模块中量化用户行为对资源的威胁，伪代码图 4 所示；

```
Input:action,action_Probability,outcome,weight_outcome,context  //用户行为、行为产生的可能性、用户行为产生的结果、结果的权重、上下文
Output:objectThreat  //用户行为对资源的预期威胁
Initialize:action←“View”,action_Probability←0.5,outcome←“Unavailable”,weight_outcome←0.8,context←0.6,objectThreat←0;  //初始化
cost_Outcome←cost_OutcomeFunction(action,outcome,context);  //结果代价函数模型
cost_Action←cost_ActionFunction(cost_Outcome,weight_outcome);  //行为代价函数模型
utility←utilityFunction(cost_Action,action_Probability);  //资源敏感度的权重即效用性函数模型
objectThreat←uobjectSecurityLevel*utility;  //权重线性回归计算用户行为对资源的预期威胁
end
Return:objectThreat;
```

图.4:AIC 模块伪代码

③建立预期理论函数模型将威胁值转为风险值。

(3)基于 XACML 对风险策略进行扩展，并根据风险值动态调整访问控制策略。

风险策略用 XML 表示，描述如何约束基于风险的访问控制方法，该文件由资源提供者创建。每个策略由资源、用户、风险因素、量化函数、风险集合函数和风险阈值组成。风险策略支持不同风险因素和量化方法的使用，它按照 XML 的结构，将风险策略作为根元素；资源、用户、风险因素、集合函数和风险阈值作为子元素。风险策略案例如表 1 所示：

表 1：一个简单风险策略的案例

```
<risk-policy version=“1.0”
xmlns:rp=“http://inf.usfc.br/danielrs/risk-policy” >
<rp:resource id=“0” />
<rp:user id=“0” />
<rp:metric-set name=“NAME” >
<rp:metric>
      <rp:name>NAME<rp:name>
      <rp:description>DESCRIPTION</rp:description>
      <rp:quantification>QUANTIFICATION</rp:quantification>
<rp:metric>
</rp:metric-set>
<rp:aggregation-function>ABC</rp:aggregation-function>
<rp:risk-threshold>99</rp:risk-threshold>
</rp:risk-policy>
```

2、技术路线

本课题是面向雾计算，围绕“如何使扩展后的 XACML 量化请求的风险”、“如何分析和量化预期威胁并转化成风险值,使其实现 XACML 执行过程中风险量化的功能”、“如何形式化风险策略”三个关键问题，拟采用以下技术路线(如图 3 所示)：

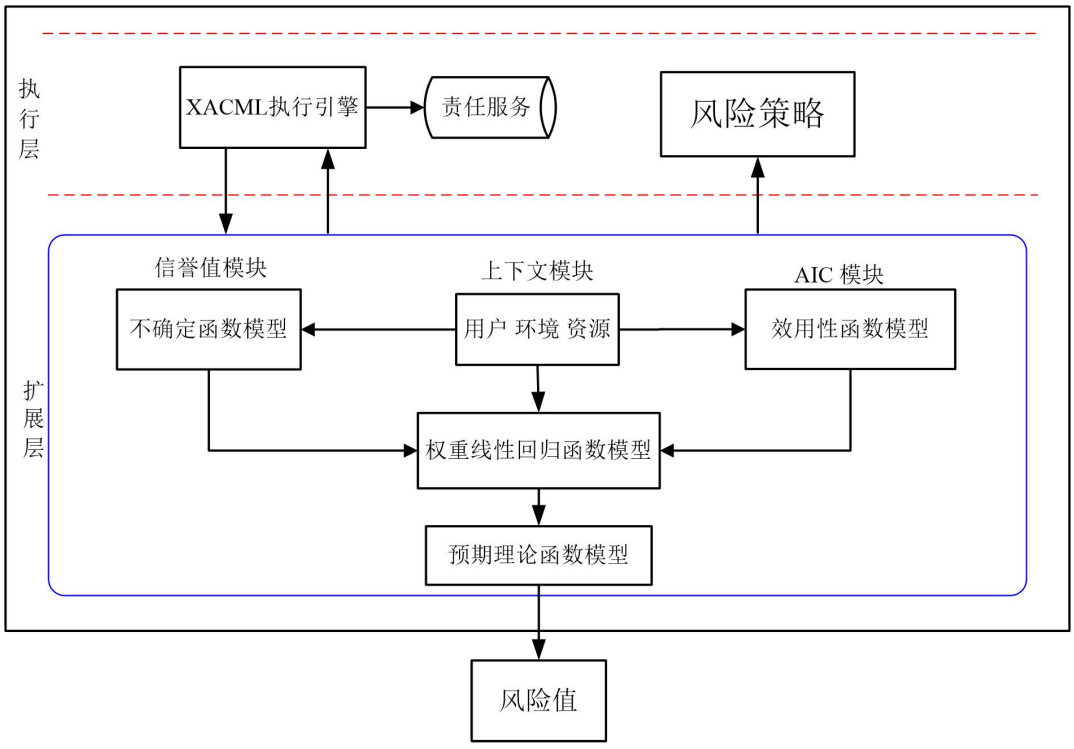

图. 3:本课题拟采取的技术路线

首先，对 XACML 组件进行扩展使其满足风险评估需求，以量化用户请求的风险；同时，对 XACML 执行引擎进行扩展，使其满足扩展后的 XACML 的执行需求；

其次，在信誉值模块中建立不确定函数模型，以量化用户访问的威胁；在 AIC 模块中建立效用性函数模型，以量化用户行为对资源的威胁；添加上下文模块以在访问过程中动态改变预期威胁。根据权重线性回归函数模型和预期理论函数模型将预期威胁转化为风险值；

再次，在 XACML 策略的基础上添加风险策略，满足访问控制策略(风险无关策略和风险相关策略)请求将被允许，并根据风险值动态调整访问控制策略；

最后，在实验平台上实现其原型系统，证明此课题的可行性和实用性。

3、可行性分析

(1)XACML 为风险评估框架提供理论和实验的基础

本课题对 XACML 组件进行扩展加入风险评估框架，还对 XACML 执行引擎进行扩展，最后基于风险评估的访问控制方法都是基于 XACML 实现的。

(2)传统的风险评估框架考虑的风险因素和函数模型为此课题的实施提供技术上的可行性

传统的风险评估框架考虑实体因素较多，例如用户和资源，本课题还考虑用户信誉值和用户行为，建立多个函数模型。

(3)传统的 XACML 策略为本课题风险策略的实现提供理论基础

本课题基于传统的 XACML 策略提出风险策略，如果满足访问控制策略(风险无关策略和风险相关策略)，请求将被允许。

(4)研究室的软、硬件、网络环境具备实验条件，可以验证提出的改进方案并且实现提出的新方案。

综上所述，本研究任务是可行的。

四、研究基础与条件

(1)研究本课题前看了以下论文：

①介绍雾计算并提出雾计算中的隐私安全[1][2][6]；

②风险评估只考虑风险的实体因素，例如用户和资源来量化风险，并没有面向用户信誉值和用户行为[3][4][7][8][9]；

③风险评估只考虑用户信誉值来量化风险，但不是面向用户行为[5][10][11][12][13][14]；

④风险评估只考虑用户信誉值和行为来量化风险，但是没有考虑用户行为产生的结果对风险值的影响[15][16][17][18][19][20][21]。

(2)代码基础：前期自己通过看书学习 java 基础知识，看论文实现算法并验证实验，还学习数据库和网络的相关知识。

(3)项目基础：本课题是基于国家自然科学基金青年项目(Grant 61602262)和江苏省自然科学基金青年项目(Grant BK20150865)研究的。

五、研究进度及具体时间安排(包括起讫日期、主要研究内容和预期结果)

1.时间安排

第一阶段 2019.07—2019.09 查阅国内外相关文献，解国内外相关研究现状及发展趋势。

第二阶段 2019.09—2019.11 确定研究的主要方向并完成开题报告。

第三阶段 2019.11—2020.03 深入调研相关领域的研究状况，进行理论分析，解要完成的工作，研究现有代码。

第四阶段 2020.04—2020.08 对论文的创新点进行建模实现，得到具体的优化方案。

第五阶段 2020.09—2020.12 论文初稿完成，征求老师和同学的意见，对论文进行修改并逐步完善。

第六阶段 2021.01—2021.02 确定论文的最终版本，准备毕业论文答辩。

2. 预期结果

1）一篇中文论文和一篇英文论文

2）毕业论文

导师对开题报告的意见

该学生对本课题进行了充分的调研，阅读了多篇具有代表性的中英文文献，并对课题有一定理解。访问控制是保证用户数据安全的重要手段之一，本课题基于传统的访问控制模型，提出了基于风险值的访问策略自动更新的方法，具有一定的理论和实用价值。研究方法与研究计划安排合理，难度适中。同意开题。

签名：柯昌博　　日期： 2019 年 11 月 14 日