分级的软件可信评估模型研究及应用

贾晓辉 张文宁 刘安战
(中原工学院软件学院 郑州 450007)

摘 要 针对软件的可信任问题,展开对软件可信程度的度量和评估的研究,提出了软件质量模型及分级的可信软件评估模型,将软件的信任程度分为存在级、不可信级、可用级、证实级、推荐级、应用级等6个可信级别。基于决策树给出了可信软件等级的评估过程,并将其应用于可信构件平台中。经过测试,系统运行稳定,对高可信软件的开发和重用具有引导作用。

关键词 软件复用,可信软件,分级,软件评估
中图法分类号 TP302.2 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.04.037

Research and Application on Software Trustworthiness Evaluation Model Based on Classification

JIA Xiao-hui ZHANG Wen-ning LIU An-zhan
(College of Software, Zhongyuan University of Technology, Zhengzhou 450007, China)

Abstract Aiming at the problem of software trustworthiness, we researched on the software quality model and the evaluation model, and put forward the software quality model and the evaluated model for software trustworthiness. The degree of software trust is divided into existing level, trustless level, useable level, corroborated level, recommended level and application level. The decision tree is used to express the evaluation process. It is applied to the trusted component platform and the system runs stably after testing, it can play a guide role in the development and reuse of high trusted software.

Keywords Software reuse, Trust-component, Classification, Software evaluation

1 引言

构件是指具有一定功能、可明确标识的软件单位,具备可复用性的特征[1]。作为提高软件生产率和软件质量的有效途径,基于构件的软件开发已经成为软件工程研究领域的重点之一[2]。目前,构件资源库的服务形式呈现出开放、高度动态和公共可访问的特性[3],加快了资源的传播速度,复用者可以更加方便和充分地利用已经存在的各类构件资源。但也正因为资源的开放性和群体的多样性,使得构件质量更加难以预测和评估,人们难以对构件的信任程度进行衡量,构件的可信性逐步成为研究热点。

鉴于高校实践教学的持续性和重复性等特征,在高校实践教学中引入构件相关理论,将学生作品视为构件,使得后续学生的实践学习能够以此软件为基础进行改进或者复用;对学生作品的可信性展开研究,希望提高知识共享度并激发学生学习兴趣,在一定程度上缓解题目单调和质量不高的问题,也有助于增强实践教学的连续性,为学生创新能力的培养奠定基础。

2 相关研究

自 Anderson 于 20 世纪 70 年代提出软件可信的概念后[4],人们从不同的研究领域和角度对软件可信的内涵及可信程度的评估进行了深入探讨,如典型的 Beth 模型、TEM 模型和 DTME 模型等。可信构件自 1998 年在"Tools Pacific 1998"会议上被正式引入软件工程领域后,便得到了人们的高度重视。目前开展的相关研究主要有构件资源的开发、构件的可信保证、软件复用与形式化开发方法的融合、面向特定场景的可信构件应用等[5],且取得了很大进展。其中,构件的质量模型是对构件进行度量和评估的基础,是研究的重中之重。目前国内外已有多个可信构件质量模型,被广泛认可的有澳大利亚 Meyer 等人于 2003 年提出的可信构件 ABCDE 模型[6],其根据构件质量特性将模型分为构件的接受性、构件行为、构件约束、构件设计、构件扩展性等 5 个类别。国内软件构件标准工作组于 2007 年给出了软件构件两部分模型:内部质量和外部质量模型、使用质量模型[7]。其中内部与外部质量模型将构件的质量属性划分为功能性、可靠性、易用性、效率、维护性、可移植性和可复用性共 7 个子特性,使用质量模型包含有效性、生产率、安全性、满意度和可信度共 5 个特性,这些模型为构件的可信和应用研究奠定了基础。在对软件可信的研究中,郎波等提出了一种软件可信分级模型[8],按照开发阶段、提交阶段、应用阶段中分别提供的不同可信证据满足

到稿日期:2015-11-30 返修日期:2016-02-23 本文受河南省科技攻关项目(152102210154),河南省高等学校重点科研项目计划(14B520054,15B520041)资助。

贾晓辉(1972—),女,硕士,副教授,主要研究方向为软件工程,E-mail:xhui_jia@163.com;张文宁(1982—),女,硕士,讲师,主要研究方向为软件工程;刘安战(1981—),男,硕士,讲师,主要研究方向为移动开发。

的不同条件，将软件分为 6 个可信级别，但其证据的可信级别系人为主观判断划分，因此会造成软件可信级别判断不统一等问题。王犇等提出了基于多属性熵权合成的软件可信等级评估方法[9]，其基于对证据分类来合成多元可信证据，然后通过不确定熵计算各可信属性的权重值，解决了软件可信性评估中可信证据合成时的证据冲突以及多属性权重分配等问题。王琦等基于云模型的电力生产管理软件可信评估方法[10]，依托电力行业，对软件的可信属性进行二级划分，并采用云模型方法实现量化，用数字特征图的形式给出了软件可信评估等级，将电力软件分为 4 个可信级别。该软件可信分级主要是针对软件本身的一些可信属性展开，没有考虑软件生产者、使用者甚至第三方等其他可信因素对软件可信的影响。

大多数质量模型从不同的角度定义了构件可信性验证的标准。但构件是为特定领域的复用需求而开发的，在开发和复用之前，必须对构件复用领域的特性进行研究分析，将领域特征和可信构件质量模型相结合，有针对性地提出与应用场景相符的质量模型[11]。

3 软件质量模型

软件可信是指软件行为符合用户预期并满足用户的需求[12]，不同学者从不同的研究领域和不同的角度对软件可信的内涵进行了研究，多数认为软件可信不仅包含软件的可用性、可靠性、安全性等服务质量及其在人们心目中的综合反映，也包括软件行为和结果与用户预期结果的一致性[1]。

软件作为一种资源，人们对其可信性提出了要求，期望软件执行与用户预期的行为和结果相一致。以高校学生实践教学为应用背景，以学生开发的软件作品为研究对象，从软件可信的内涵出发，结合高校实践教学的特点，形成面向高校实践教学的可信软件质量模型及评估模型，如表 1 所列。

表 1 构件质量模型

一级指标	二级指标	说明
功能性	适合性	软件为特定任务或目标提供的一组合适的功能的能力
	准确性	软件提供正确结果或效果的能力
	互操作性	软件与一个或其他构件和系统进行交互的能力
	保密安全性	软件保护信息和数据的能力
易用性	易理解性	使用户能理解软件是否合适及如何能将软件用于特定的任务的能力
	易学性	使用户能学习和使用软件的能力
	易分析性	使用户能分析软件并在此基础上进行优化的能力
	易操作性	用户能操作和控制软件的能力
可靠性	容错性	在软件出现故障或者违反其指定接口的情况下，软件维持规定的性能级别的能力
	测试充分性	软件被测试的充分程度，说明其健壮性的能力
	稳定性	软件避免由于修改而造成意外结果的能力
	防抵赖性	软件生产者对软件发布等行为的不可不承认性
可复用性	规范性	软件及其支撑资料符合相关规定的能力
	接口成熟性	软件产品提供某种服务且完成其逻辑行为的能力
	独立性	在要求的运行环境下，软件产品不依赖其他环境而能独立工作的程度
	通用性	软件产品所应用的领域或应用平台覆盖面的广度
	易组装型	软件在一定环境下与其他构件结合的能力

构件质量模型是关于构件自身质量的质量特性。从构件自身的客观角度和高校实践环节的应用场景来看，一个良好的构件除了具有可复用性的本质特征外，还应满足学生对构件的可用性、完整性和支撑材料完备性的预期期望。面向实践环节的构件质量模型进一步分为功能性、易用性、可靠性和可复用性共 4 个质量特性。功能性是指构件在指定条件下使用时满足明确和隐含要求功能的能力，具体包括功能实现的适合性、准确性、互操作性和保密安全性 4 个子特性；易用性是指构件在指定条件下使用时被理解、学习、使用和吸引用户的能力，包括构件及其支撑材料的易理解性、易学性、易分析性和易操作性 4 个子特性；可靠性指构件维持规定的功能或性能水平的能力，也即在规定的条件下及规定的时间内无失效运行的能力，包括构件的容错性、测试充分性、稳定性和防抵赖性 4 个子特性；可复用性是为支持构件的修改、修正、改进、优化等复用工作提供的支持程度，包括规范性、接口成熟性、独立性、通用性和易组装性 5 个子特性[10]。

4 可信软件评估模型

软件可信性是软件使用者对软件的功能性、易用性、可靠性、可复用性等不同方面的主观感受；软件可信评估是对这种主观感受以量化方式进行客观表达，根据可信属性的满足程度对软件进行分级。

4.1 软件可信等级模型

软件的可信等级主要是根据软件本体、本体证据、用户评价、专家评价等条件进行判断。不同级别的软件符合不同的等级要求。

定义 1(软件本体) 软件本体指构成软件的计算机程序、执行库及描述软件的基本信息，如名称、版本、开发者、发布日期等，用 C 表示。

定义 2(本体证据) 为一个软件提供的证明依据，包括软件的分析设计文档、测试报告等，用 B 表示。一个软件 C 的本体证据用 $B(C)$ 表示。

定义 3(可信评价) 表示一个软件 C 在某一级别层次上通过收集来自生产者、消费者和第三方等的度量数据，结合系统的评价机制对该软件的综合度量，第 i 级可信级别使用 $Ei(C)$ 表示，其中 $1\leqslant i\leqslant N$。

定义 4(综合评价) 使用者、生产者、专家等对软件属性的加权度量，用 $A(C)$ 表示。

定义 5(升级阈值) 一个软件从第 $i-1$ 级升级到第 i 级的有效条件，称为第 i 级的升级阈值，用 T_i 表示。

定义 6(可信级别) 表示软件可信度的级别，一个可信模型可以定义 N 个级别，第 i 级可信用 G_i 表示，其中 $1\leqslant i\leqslant N$。

定义 7(可信集) 属于某一可信级别的所有软件的集合，用 S 表示，$S(G_i)$ 表示所有第 i 级可信构件组成的可信集。

定义 8(活跃度) 用户上传、下载、评论构件的数量。

综合所有定义，软件集合 $S(G_1)\supset\cdots\supset S(G_i)\supset\cdots\supset S(G_n)$，其中 $1\leqslant i\leqslant N$。假设 $C\in S(G_{i-1})$，当 E_i 超过 T_i 时，则 $C\in S(G_i)$。

4.2 分级的可信软件

针对学生在实践教学环节过程中开发时间短而导致的大

多数项目不完善等特点，将软件可信级别定义分为 6 个，分别为存在级 $G1$、不可用级 $G2$、可用级 $G3$、证实级 $G4$、推荐级 $G5$ 和应用级 $G6$，如图 1 所示。

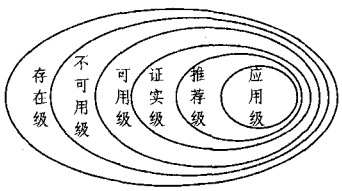

图 1　构件可信等级

1）存在级（$G1$）：构件 C 一旦产生，则根据定义 7，$C\in S(G1)$；

2）不可用级（$G2$）：若构件 $C\in S(G1)$，且存在经过证实的举报，则根据定义 7，$C\in S(G2)$；

3）可用级（$G3$）：若构件 $C\in S(G2)$，当其存在 $B(C)$ 并且可信评价 $E3$ 超过 $T2$ 时，则根据定义 7，$C\in S(G3)$；

4）证实级（$G4$）：若构件 $C\in S(G3)$，当其存在专家推荐并且可信评价 $E4$ 超过 $T3$ 时，则根据定义 7，$C\in S(G4)$；

5）推荐级（$G5$）：若构件 $C\in S(G4)$，当其下载排名在设定的阈值之外并且评价其 $E5$ 超过 $T4$ 时，则根据定义 7，$C\in S(G5)$；

6）应用级（$G6$）：若构件 $C\in S(G5)$，当其下载排名在设定的阈值之内并且评价其 $E6$ 超过 $T5$ 时，则根据定义 7，$C\in S(G6)$。

4.3　软件可信评估算法

软件的可信评估通过收集、分析和整理来自软件发布者、使用者、第三方及软件本体等多方面的度量数据，将各度量值依据评估过程映射到可信等级。软件的可信等级取决于投诉、本体证据、专家推荐、下载排名、综合评价等多个条件。下载排名可以根据需要来确定阈值。综合评价由对用户的评价和对软件的评价两部分组成，其中对用户的评价包含用户类型、基本信息、可信证据、活跃度等 4 个方面，对构件的评价包含构件的功能性、易用性、可靠性、可复用性 4 个方面。

软件的可信根据是否有处理的投诉、是否具备软件的本体证据、是否有专家推荐、下载排名是否在一定阈值之内、综合评价得分等选项综合确定。

综合评价用 P_c 表示，计算公式如下：

$$P_c=U\times P_{(u,c)}$$

其中，U 代表用户可信度量向量，$P_{(u,c)}$ 代表用户对构件 c 的可信评价向量。

$U=(u_1\cdots u_i\cdots u_n)$，$u_i$ 代表第 i 个用户的可信度量。

这里把所有的用户分为 m 个类型用户集合，$S(j)$ 表示第 j 个类型的所有用户集合，$1\leqslant j\leqslant m$。

用 W_j 表示第 j 类用户集合的权重，对于任意一个 u_i 属于 $S(j)$，有：

$$u_i=\frac{W_j}{|S(j)|}(V_{(u_i,b)}+V_{(u_i,t)}+V_{(u_i,a)})$$

其中，$|S(j)|$ 表示集合元素个数，$V_{(u_i,b)}$ 表示用户 u_i 的基本信息可信度量，$V_{(u_i,t)}$ 表示用户 u_i 的认证信息可信度量，$V_{(u_i,a)}$ 表示用户 u_i 的活跃度信息可信度量。

$$P_{(u,c)}=\begin{pmatrix}P_{(u_1,c)}\\ \cdots\\ P_{(u_i,c)}\\ \cdots\\ P_{(u_n,c)}\end{pmatrix}$$

其中，$P_{(u_i,c)}$ 表示用户 u_i 对构件 c 的评价。假设构件 c 有 k 个评价指标，那么用户 u_i 对该构件的评价计算公式为：

$$P_{(u_i,c)}=\sum_{j=1}^{k}W_j\times P_{(u_i,c,j)}$$

其中，$P_{(u_i,c,j)}$ 表示用户 u_i 对构件 c 的第 j 个指标的评价，W_j 表示该构件的第 j 个指标的权重。

评价模型如图 2 所示，最终的构件评价结果为存在级、不可用级、可用级、证实级、推荐级和应用级中的一种。

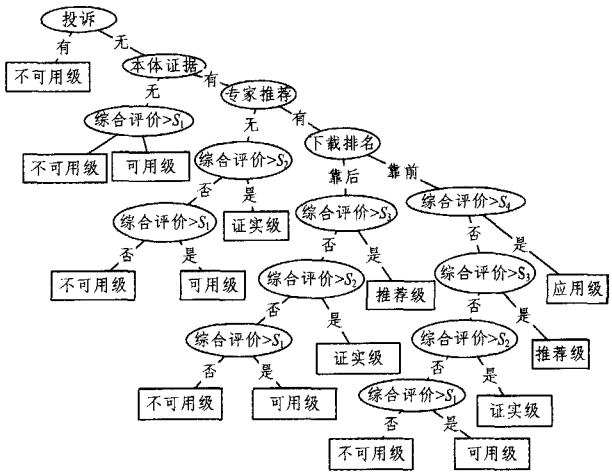

图 2　软件可信评估树

该算法完全支持软件可信级别的动态计算和调整，便于实施。基于该算法思想实现对可信软件的管理，以达到对用户信用管理、软件全生命周期度量数据的收集和计算以及基于实时数据的可信等级的动态计算。

4.4　分级的可信软件评估模型的应用

软件的评价指标根据用户对构件的评价加权计算得出，结合可信构件平台的应用场景，采用优序图法。根据用户与构件的关系将用户主要分为 3 类，分别是构件使用者、构件生产者、专家。用户类型优序结果如表 2 所列，权重结果如表 3 所列。

表 2　用户可信类型计算

	生产者	使用者	专家	得分
生产者	0.5	0	0	0.5
使用者	1	0.5	0	1.5
专家	1	1	0.5	2.5

表 3　用户可信类型权重

指标	权重
生产者	0.11
使用者	0.33
专家	0.56

用户的可信指标由基本信息、可信认证、活跃度等因素组成，其中基本信息、可信认证、活跃度是指标的优序列表，如表 4 所列；用户的可信指标权重如表 5 所列。

表 4 用户可信指标计算结果

	基本信息	可信认证	活跃度	得分
基本信息	0.5	1	1	2.5
可信认证	0	0.5	1	1.5
活跃度	0	0	0.5	0.5

表 5 用户可信指标权重

指标	权重
活跃度	0.11
可信认证	0.33
基本信息	0.56

软件的评价指标按重要程度顺序为功能性、软件易用性、软件的可靠性、软件可复用性、软件的可信证据。计算得到专家类型的权重为 56%，使用者类型的权重为 33%，生产者类型的权重为 11%。同理计算得到软件的功能性指标权重为 36%，易用性指标权重为 28%，可靠性权重指标为 20%，可复用性指标权重为 12%，可信证据的权重为 4%。软件指标优序计算结果如表 6 所列，指标权重如表 7 所列。

表 6 软件指标计算结果

	功能性	易用性	可靠性	可复用性	得分
功能性	0.5	1	1	1	3.5
易用性	0	0.5	1	1	2.5
可靠性	0	0	0.5	1	1.5
可复用性	0	0	0	0.5	0.5

表 7 软件指标权重

指标	权重/%
功能性	44
易用性	31
可靠性	19
可复用性	6

设置软件排名的阈值为 0.20，即前 20%定义为排名靠前的分支。在软件可信评估模型中，设置 $S1=60$，$S2=70$，$S3=80$，$S4=90$，因此不可用级别软件综合评价得分在 0～59 之间，可用级别软件综合评价得分在 60～69 之间，证实级别软件综合评价得分在 70～79 之间，推荐级别软件综合评价得分在 80～89 之间，应用级别软件综合评价得分在 90 及以上。该算法已应用在可信软件管理平台中。

结束语 目前基于重用的构件开发思想已日益成熟并得到广泛应用，然而高校教育教学过程中基本沿用从零开始构造软件的开发方法，大多开发成果因为项目不成熟并未得到推广利用。在分析高校实践环节运行特点的基础上，将可信软件、构件等相关理论运用于学生实践教学环节中。在研究目前常用软件、构件质量模型的基础上，提出了与实际应用场景相符合的软件质量模型，指出软件的可信属性包含功能性、易用性、可靠性和可复用性 4 个方面，是软件质量的全方位体现。定义了存在级、不可用级、可用级、证实级、推荐级和应用级共 6 个可信软件级别，对给定软件的可信等级进行判定的方法是一个依据度量数据从判定树的树根到叶子结点的深度搜索过程，且时间复杂度较小，便于实施和应用。关于该判定树的进一步效率分析、优化和具体应用将在下一步研究中开展。

参 考 文 献

[1] WANG Y H, ZENG G P. Research on Trust Evaluation Model for Component Assets based on Fuzzy Sets [J]. Application Research of Computers, 2014, 31(5): 1467-1474. (in Chinese)
汪永好，曾广平. 基于模糊集合的构件资源信任评估模型研究[J]. 计算机应用研究，2014，31(5)：1467-1474.

[2] GUO S H, LAN Y Q, JIN M Z. Some Issues about Trusted Components Research[J]. Computer Science, 2007, 34(5): 243-246. (in Chinese)
郭树行，兰雨晴，金茂忠. 软件构件的可信保证研究[J]. 计算机科学，2007，34(5)：243-246.

[3] CAI S B, ZOU Y Z, SHAO L S, et al. Framework Supporting Software Assets Evaluation on Trustworthiness [J]. Journal of Software, 2010, 21(2): 359-372. (in Chinese)
蔡斯博，邹艳珍，邵凌霜，等. 一种支持软件资源可信评估的框架[J]. 软件学报，2010，21(2)：359-372.

[4] ZHOU J, ZHANG M X. Survey on Trustworthy Software Evaluation[J]. Application Research of Computers, 2012, 29(10): 3609-3613. (in Chinese)
周剑，张明新. 软件可信评估综述[J]. 计算机应用研究，2012，29(10)：3609-3613.

[5] WEI L, ZHAO Q Y, SHU H P. A Trusted Component Choosing Method Based on Scene Matching[J]. Microelectronics & Computer, 2011, 28(8): 176-179. (in Chinese)
魏乐，赵秋云，舒红平. 一种基于场景匹配的可信构件选择方法[J]. 微电子学与计算机，2011，28(8)：176-179.

[6] SI G N, XU J, YANG J F, et al. An evaluation model for dependability of internet-scale software on basis of Bayesian networks and trustworthiness[J]. Journal of Systems and Software, 2014, 89: 63-75.

[7] SJ/T11374-2007，软件构件产品质量第 1 部分质量模型[S]. 中国：软件构件标准工作组，2007.

[8] LANG B, LIU X D, WANG H M, et al. A Classification Model for Software Trustworthiness[J]. Journal of Frontiers of Computer Science and Technology, 2010, 4(3): 231-239. (in Chinese)
郎波，刘旭东，王怀民，等. 一种软件可信分级模型[J]. 计算机科学与探索，2010，4(3)：231-239.

[9] WANG B, ZHOU X S, YANG Y L. An Entropy-weighted Multi-attribute Combination Method for Software Trustworthiness Classification Assessment[J]. Microelectronics & Computer, 2014, 31(6): 21-24. (in Chinese).
王犇，周兴社，杨亚磊. 基于多属性熵权合成的软件可信等级评估方法[J]. 微电子学与计算机，2014，31(6)：21-24

[10] WANG Q, WANG Y B, CAO Y Z. Dependability Assessment Method of Electric Production Management Software Based on Cloud Model[J]. Computer Applications and Software, 2012, 29(7): 33-45. (in Chinese)
王琦，王永滨，曹轶臻. 基于云模型的电力生产管理软件可信评估方法[J]. 计算机应用与软件，2012，29(7)：33-45.

[11] DING B, WANG H M, SHI D X, et al. Component Model Supporting Trustworthiness-Oriented Software Evolution[J]. Journal of Software, 2011, 22(1): 17-27(in Chinese).
丁博，王怀民，史殿习，等. 一种支持软件可信演化的构件模型[J]. 软件学报，2011，22(1)：17-27.

[12] LI X L, LIU C, JIN M Z, et al. Software Component Reusability Quality Metrics[J]. Application Research of Computers, 2007, 24(6): 280-283. (in Chinese)
李晓丽，刘超，金茂忠，等. 软件构件的可复用性质量度量[J]. 计算机应用研究，2007，24(6)：280-283.