基于熵权系数法的信息安全模糊风险评估

罗 佳,杨世平
(贵州大学 计算机科学与技术学院,贵州 贵阳 550025)

摘 要:信息安全风险分析中存在大量模糊、不确定性影响因素,以往的信息安全风险综合分析方法如PRA分析法需要收集到精确全面的评估数据,通过故障树分析信息系统被攻击的原因,建立风险计算模型定量计算系统风险,此方法过于繁琐,不易对信息系统风险进行准确的量化。针对此问题,文中通过对信息系统风险影响因素的识别与分析,构建反映信息安全风险影响因素及它们相互关系的风险评估指标体系,并应用多级模糊综合评判法对风险评估指标进行多层量化评估,同时利用信息熵定量计算各风险影响因素的权重,克服了直接赋值的主观性。该方法能较好地量化评估信息系统风险,方便计算出信息系统总的风险值。

关键词:信息安全;风险评估指标体系;安全事件;模糊综合评判;熵权系数;风险分析
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2009)10-0177-04

Fuzzy Risk Assessment for Information Security Based on Method of Entropy-Weight Coefficient

LUO Jia, YANG Shi-ping
(College of Computer Science and Technology, Guizhou University, Guiyang 550025, China)

Abstract: There are a lot of fuzzy and uncertain factors in the course of information security risk analysis, the previous information security risk analysis methods, such as PRA analysis method, which need to collect accurate and overall assessment data. Through the fault tree analyze the causes of information system were attacked, establish the model of risk calculation to quantitative calculation the system risk, this method is too complicated. To solve this problem, based on information system risk factors, the recognition and analysis of information system risk factors of affecting reflects the inter-relationship to build their risk evaluation index system, and the application of multi-grade fuzzy comprehensive evaluation method for risk assessment index system, at the same time, using the quantitative evaluation multi-layer quantitative calculation of information entropy weight of each risk factors for overcoming the subjectivity of the direct assignment. Practice proves that this method can better quantitative evaluation information system risk, calculate the total value of information system risk.

Key words: information security; risk evaluation index system; security event; fuzzy comprehensive judgment; entropy-weight coefficient; risk analysis

0 引 言

信息安全风险评估是信息安全等级保护管理的基础工作,是信息安全风险管理的重要环节。通过开展信息安全风险评估,对网络与信息系统的资产价值,潜在的安全威胁、薄弱环节、防护措施等进行分析,可以发现信息系统中存在的主要安全问题,并找到解决这些问题的方法,有针对性地进行管理[1]。一个内容全面、逻辑清晰的信息安全风险评估指标体系是有效量化评估风险的前提。目前,还未建立比较全面的信息安全风险评估指标体系,许多风险评估指标体系未对风险的本质、结构及构成要素做出客观的描述。一些评估指标体系,仅把资产、威胁、脆弱性作为评估指标,实际上它们也受多种因素影响,需要分层细化。另一些把系统常见的几种威胁、脆弱性种类作为威胁、脆弱性的下层评估指标。由于信息系统的复杂性,其面临的风险会随着客观条件的变化而变化,当然威胁源、威胁行为、脆弱性也随之改变,所以不能准确地量化评估风险。信息安全风险由安全事件发生的可能性及其产生的影响两个指标来衡量[2]。量化风险的重点是量化安全事件发生的频率及发生后的影响[3]。文中通过对安全事件发生可能性及其产生影响的因素集进行全面

收稿日期:2009-02-26;**修回日期**:2009-05-16
基金项目:贵州省科学技术基金项目(黔科合J字[2007]2204号)
作者简介:罗 佳(1983-),女,贵州毕节人,硕士研究生,研究方向为网络与信息安全;杨世平,教授,研究方向为计算机网络安全。

的分析,分层细化,分别建立安全事件发生可能性及其产生影响的评估指标体系,应用模糊综合评判法分层量化评估它们的值,最终计算出系统风险值。

1 信息安全风险分析及其计算方法

1.1 信息安全风险分析

风险分析中要涉及资产、威胁、脆弱性等基本要素[1]。每个要素有各自的属性,资产的属性是资产价值;威胁的属性可以是威胁主体,出现的频率、动机等;脆弱性的属性是被威胁利用的难易程度。风险分析的主要内容为:

1) 对资产识别,并对资产的价值赋值。

2) 对威胁识别,描述威胁的属性,并对威胁出现的频率赋值。

3) 对资产的脆弱性识别,并对脆弱性的严重程度赋值。

4) 根据威胁发生可能性及脆弱性被利用的难易程度判断安全事件发生的可能性。

5) 根据脆弱性的严重程度及安全事件作用资产的价值计算安全事件的损失。

1.2 信息安全风险的计算方法

信息系统风险是安全事件发生概率及其后果的函数[4],若已知安全事件发生概率及后果的函数,则关于风险的计算为:

$$R(x) = R(p,c) = \sum_{i=1}^{n} p_i u(c_i) \quad (1)$$

x 为系统风险,$c = (c_1 \cdots c_i)^T$,$p = (p_1 \cdots p_i)^T$,c_1,$\cdots c_i$ 表示安全事件造成的 n 个后果,$p_1 \cdots p_i$ 表示 c_1,$\cdots c_i$ 发生的概率且 $\sum_{i=1}^{n} p = 1$,$u(c_i)$ 表示后果价值的量化函数,因此,安全事件发生的可能性及其造成的损失决定了风险的计算。

2 构建信息安全风险评估指标体系及风险因素权重的确定

2.1 构建信息安全风险评估指标体系

风险是潜在安全事件发生的可能性及其产生的影响,可见风险与安全事件是紧密相关的,量化风险实际上就是量化安全事件发生的可能性和其产生的影响[5]。因此通过对安全事件发生可能性及其产生影响的影响因素进行分析,分层细化,分别建立安全事件发生可能性和发生后产生影响的评估指标体系。安全事件发生的可能性主要由威胁发生的概率、脆弱性、安全措施的有效性三项指标决定。安全事件产生后的影响主要通过对信息系统资产价值、系统能力及恢复费用三项指标衡量。威胁发生的可能性指标主要划分为:威胁源的行为动机,技术力量,拥有的资源,风险承受能力,受惩罚的可能性,资产对威胁源的吸引力。脆弱性主要由系统脆弱性的暴露程度及被威胁利用的难易程度来决定,安全措施有效性从安全技术有效性和安全管理策略有效性来评价。信息系统资产的价值由资产的机密性、完整性、可用性三项属性来衡量。系统能力的影响主要表现为削弱,延迟,中断;恢复费用主要为信息恢复,服务恢复。

安全事件发生可能性和发生后产生影响的评估指标体系分别如图 1、图 2 所示。

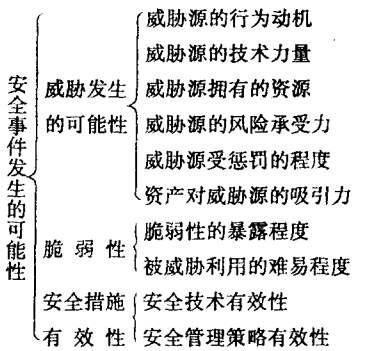

图 1 安全事件发生可能性的评估指标体系

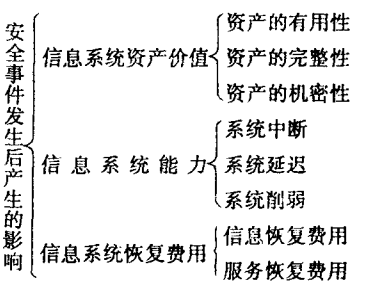

图 2 安全事件发生后产生影响的评估指标体系

2.2 风险因素权重的确定

确定权重的常用方法有 AHP 分析法、统计试验法等。为了在主观赋权的基础上反映客观要求的权重,采取熵权系数法,通过定量计算各因素的权重[6]。

2.2.1 熵的性质

熵是系统不确定性的度量。假如系统处于不同的状态下的概率为 $p_1, p_2, \cdots, p_n$,则系统的熵为 $H = -\sum_{i=1}^{n} P_i L_n P_i$,其中 $\sum_{i=1}^{n} P_i = 1$,当系统概率 $P_i = 1/n$ 时,熵最大 $H = L_n n$。

2.2.2 确定风险因素的熵权系数

信息熵 $H = -\sum_{i=1}^{n} P_i L_n P_i$,表示系统的有序程度,由熵极值性知,$P_i$ 越接近相等,熵值越大,风险因素对系统风险影响的不确定性就越大[7]。因此,可用信息熵计算各风险因素的权值。根据风险因素对评判集中各指标的支持度 r_{ij},利用信息熵计算各指标的权重。

风险因素 U_i 的相对重要性由下列熵来度量:

$$H_i = -\sum_{j=1}^{m} r_{ij} L_n r_{ij} \tag{2}$$

当 $r_{ij}(j = 1,2,\cdots,m)$ 取值相等时,熵最大为 $L_n m$,用 $L_n m$ 对公式(2)进行归一化处理,可得衡量风险因素相对重要性的熵值为:

$$e_i = -\frac{1}{L_n m}\sum_{j=1}^{m} r_{ij} L_n r_{ij} \tag{3}$$

由于熵最大时,风险因素对系统风险评估的贡献最小,因此确定风险因素的权重可由 $1 - e_i$ 来度量[4]。对其进行归一化得到风险因素 U_I 的权重 Φ_i 为:

$$\Phi_i = -\frac{1}{n - E}(1 - e_i) \tag{4}$$

其中 $E = \sum_{i=1}^{n} e_i, 0 \leqslant \Phi_i \leqslant 1, \sum_{i=1}^{n} \Phi_i = 1$。

3　模糊综合评判法的思想及其算法过程

3.1　模糊综合评判法的思想

模糊综合评判法是建立在模糊数学基础上将一些边界不清、不易量化的因素进行综合评估的方法,它特别适合用来解决那些只能用模糊的、非定量的难以明确定义的实际问题[8]。

模糊综合评判法的思想是在确定评价因素,因子的评价等级标准和权值的基础上运用模糊集合变换原理,以隶属度描述各因素及因子的模糊界限,构造模糊评价矩阵,通过一层或多层复合运算,确定评价对象所属等级。

3.2　模糊综合评判法的算法过程

根据评判因素的层次可分为一级模糊综合评判和多级模糊综合评判。多级模糊综合评判是多个一级模糊综合评判的复合。二级模糊综合评判的算法过程如下[9]:

1)确定评判对象的因素集 $U = (u_1, u_2, \cdots, u_n)$,将其分为若干组 $U = (u_1, u_2, \cdots, u_k)$,使得 $U = \bigcup_{i=1}^{k} U_i, U_i \cap U_j = \varnothing (i \neq j)$,称 $U = (U_1, U_2, \cdots, U_k)$ 为第一级因素集,$U_i = (u_1^i, u_2^i, \cdots, u_{n_i}^i)$ 为第二级因素集 $(i = 1,2,\cdots,k)$,其中 $\sum_{i=1}^{k} n_i = n$。

2) 确定评判集 $V = \{v_1, v_2, \cdots, v_m\}$。

3) 确定评判对象的单因素评判矩阵。

首先对第二级因素集 $U_i = \{u_1^i, u_2^i, \cdots, u_{n_i}^i\}$ 的 n_i 个因素进行单因素评判,即建立模糊映射:$\underset{\sim}{f_i}: U_i \to F(V)$,使得:

$u_{n_i}^i \mapsto \underset{\sim}{f_i}(u_{n_i}^i) = (r_{n_i 1}^i, r_{n_i 2}^i, \cdots, r_{n_i m}^i)$,则单因素评判矩阵为:

$$\boldsymbol{R}_i = \begin{bmatrix} r_{11}^i & r_{12}^i & \cdots & r_{1m}^i \\ r_{21}^i & r_{22}^i & \cdots & r_{2m}^i \\ \cdots & \cdots & \cdots & \cdots \\ r_{n_i 1}^i & r_{n_i 2}^i & \cdots & r_{n_i m}^i \end{bmatrix} (i = 1,2,\cdots,k)$$

r_{Lj}^i 表示因素集 u_i 中任意一个元素 u_L^i 对评判集中任一个元素的 v_j 的隶属度,确定 r_{Lj}^i 时常用德尔菲法即专家评判法。请 m 个专家评判组成小组,若对 u_i 中任意一个元素 u_L^i,有 v_{Lj}^i 个专家认为隶属于 v_j,则:

$$r_{Lj}^i = v_{Lj}^i / m (j = 1,2,\cdots,m; i = 1,2,\cdots,k; L \leqslant k) \tag{5}$$

4) 确定评判因素的权重集。

常用的方法有 AHP 分析法、统计试验法、熵权系数法等。二级评判因素集 $U_i = \{u_1^i, u_2^i, \cdots, u_{n_i}^i\}$ 的权重为:$\underset{\sim}{A_i} = \{a_{i1}, a_{i2}, \cdots, a_{in_i}\}$,一级评判因素集 $U_i = \{U_1, U_2, \cdots, U_k\}$ 的权重为:$\underset{\sim}{A_i} = \{a_1, a_2, \cdots, a_k\}$。

5) 综合评判。

首先进行二级综合评判,根据二级评判因素集 $U_i = \{u_1^i, u_2^i, \cdots, u_{n_i}^i\}$ 的评判矩阵 $\boldsymbol{R}_i$ 及 $\underset{\sim}{A_i} = \{a_{i1}, a_{i2}, \cdots, a_{in_i}\}$ 可得二级综合评判为:

$$\underset{\sim}{A_i} \circ \boldsymbol{R}_i = \underset{\sim}{B_i} (\text{其中}\circ\text{为模糊合成算子}) \tag{6}$$

然后再根据一级评判因素集 $U_i = \{U_1, U_2, \cdots, U_k\}$ 的单因素评判矩阵 $\boldsymbol{R} = (\underset{\sim}{B_1}, \underset{\sim}{B_2}, \cdots, \underset{\sim}{B_k})^{\mathrm{T}}$ 级权重集 $\underset{\sim}{A_i} = (a_1, a_2, \cdots, a_k)$ 可得到一级综合评判为:

$$\underset{\sim}{A} \circ \boldsymbol{R} = \underset{\sim}{B} (\text{其中}\circ\text{为模糊合成算子}) \tag{7}$$

6) 评判结果。

利用综合评判得到的 $\underset{\sim}{B}$ 对评判结果做出判定。常用的判定准则有最大隶属度原则和加权平均原则,为避免综合实效,均衡考虑各因素权重,通常采用加权平均原则,量化评判结果为:

$$L = \sum_{i=1}^{k} v_i b_i^n / \sum_{i=1}^{k} b_i^n (n = 1 \text{ 或 } n = 2) \tag{8}$$

4　信息安全风险的多级模糊综合评判

假设信息系统正面临某一风险,根据图 1 可知风险的安全事件发生可能性的多级模糊综合评判如下:

1) 确立评判风险的因素集 $U = \{$威胁源的行为动机,威胁源的技术力量,威胁源拥有的资源,威胁源的风险承受力,威胁源受惩罚的程度,资产对威胁源的吸引,脆弱性的暴露程度,脆弱性被威胁利用的难易程度,安全技术有效性,安全管理策略有效性$\}$,$U = \{U_1, U_2, U_3\} = \{$威胁发生的可能性,脆弱性,安全的措施有效性$\}$,$U_1 = \{$威胁源的行为动机,威胁源的技术力量,威胁源拥有的资源,威胁源的风险承受力,威

胁源受惩罚的程度,资产对威胁源的吸引}={u_1^1,u_2^1,u_3^1,u_4^1,u_5^1,u_6^1},U_2={脆弱性的暴露程度,脆弱性被威胁利用的难易程度}={u_1^2,u_2^2},U_3={安全技术有效性,安全管理策略有效性}={u_1^3,u_2^3}。

2) 确立评判因素集 $V=\{v_1,v_2,v_3,v_4,v_5\}$={很低,低,中,高,极高}。

3) 设 U_1,U_2,U_3 的单因素评判矩阵分别为 $\boldsymbol{R}_1$,$\boldsymbol{R}_2$,$\boldsymbol{R}_3$,确立隶属度 $r_{Lj}^i(i=1,2,3;\ j=1,2,3,4,5)$时采用德尔菲法请 10 个专家组成评判小组,若对 U_1,U_2,U_3 中的任意一个元素 $u_L^i(i=1,2,3)$ 有 m 个专家评判为 $v_j(j=1,2,3,4,5)$,根据公式(5)可得:

$r_{Lj}^i=m/10$ $(i=1,2,3;j=1,2,3,4,5)$,则 $\boldsymbol{R}_1$,$\boldsymbol{R}_2$,$\boldsymbol{R}_3$ 分别为:

$$\boldsymbol{R}_1=\begin{bmatrix} r_{11}^1 & r_{12}^1 & r_{13}^1 & r_{14}^1 & r_{15}^1 \\ r_{21}^1 & r_{22}^1 & r_{23}^1 & r_{24}^1 & r_{25}^1 \\ r_{31}^1 & r_{32}^1 & r_{33}^1 & r_{34}^1 & r_{35}^1 \\ r_{41}^1 & r_{42}^1 & r_{43}^1 & r_{44}^1 & r_{45}^1 \\ r_{51}^1 & r_{52}^1 & r_{53}^1 & r_{54}^1 & r_{55}^1 \\ r_{61}^1 & r_{62}^1 & r_{63}^1 & r_{64}^1 & r_{65}^1 \end{bmatrix}$$

$$\boldsymbol{R}_2=\begin{bmatrix} r_{11}^2 & r_{12}^2 & r_{13}^2 & r_{14}^2 & r_{15}^2 \\ r_{21}^2 & r_{22}^2 & r_{23}^2 & r_{24}^2 & r_{25}^2 \end{bmatrix}$$

$$\boldsymbol{R}_3=\begin{bmatrix} r_{11}^3 & r_{12}^3 & r_{13}^3 & r_{14}^3 & r_{15}^3 \\ r_{21}^3 & r_{22}^3 & r_{23}^3 & r_{24}^3 & r_{25}^3 \end{bmatrix}$$

4) 设{u_1^1,u_2^1,u_3^1,u_4^1,u_5^1,u_6^1},{u_1^2,u_2^2},{u_1^3,u_2^3}的权重分别为$(a_{11},a_{21},a_{31},a_{41},a_{51},a_{61})$,$(a_{12},a_{22})$,$(a_{13},a_{23})$根据公式(2),(3),(4)可求得。

5) 由$(a_{11},a_{21},a_{31},a_{41},a_{51},a_{61})$,$(a_{12},a_{22})$,$(a_{13},a_{23})$及 $\boldsymbol{R}_1,\boldsymbol{R}_2,\boldsymbol{R}_3$,则二级综合评判为:

根据公式(6)用模型 $M(\cdot,+)$计算得:

$\underset{\sim}{B}_1=(a_{11},a_{21},a_{31},a_{41},a_{51},a_{61})\cdot\boldsymbol{R}_1=(b_{11},b_{12},b_{13},b_{14},b_{15})$

$\underset{\sim}{B}_2=(a_{12},a_{22})\cdot\boldsymbol{R}_2=(b_{21},b_{22},b_{23},b_{24},b_{25})$

$\underset{\sim}{B}_3=(a_{13},a_{23})\cdot\boldsymbol{R}_3=(b_{31},b_{32},b_{33},b_{34},b_{35})$

$U=\{U_1,U_2,U_3\}$的单因素评判矩阵 $\boldsymbol{R}=(\underset{\sim}{B}_1,\underset{\sim}{B}_2,\underset{\sim}{B}_3)^T$,由公式(2),(3),(4)可求得权重为$(a_1,a_2,a_3)$,则一级综合评判为:

根据公式(7)用模型 $M(\cdot,+)$计算得:

$\underset{\sim}{B}=(a_1,a_2,a_3)\cdot\boldsymbol{R}=\{b_1,b_2,b_3,b_4,b_5\}$

6) 评判结果采用加权评价原则来量化评价结果,对评级集赋值 $V=\{0.1,0.3,0.5,0.7,0.9\}$,根据公式(8)可求得:

安全事件发生可能性 $L_p=\sum_{i=1}^{5}v_ib_i/\sum_{i=1}^{5}b_i(n=1;j=1,2,3,4,5)$。

风险安全事件发生后产生影响,根据图 2 可知因素集 U'={资产的完整性,资产的可用性,资产的机密性,系统中断,系统延迟,系统削弱,信息恢复费用,服务恢复费用}

$U'=\{U'_1,U'_2,U'_3\}$={信息系统资产价值,信息系统能力,信息系统恢复费用},U'_1={资产的完整性,资产的可用性,资产的机密性},U'_2={系统中断,系统延迟,系统削弱},U'_3={信息恢复费用,服务恢复费用},评判集 $V'=\{v'_1,v'_2,v'_3,v'_4,v'_5\}$。

同理根据风险安全事件发生可能性的评判步骤1),2),3),4),5)可以得到评判集 $\underset{\sim}{B}'=(b'_1,b'_2,b'_3,b'_4,b'_5)$,对评级集赋值 $V'=\{0.1,0.3,0.5,0.7,0.9\}$,根据公式(8)可以得到:

安全事件发生后产生影响 $L_p=\sum_{i=1}^{5}v'_ib'_i/\sum_{i=1}^{5}b'_i$

由公式(1)可求得风险值 $\boldsymbol{R}=L_p\times L_c$

因此,系统面临的每个风险可根据多级模糊综合评判得到量化的风险值,记为$(R_1,R_2,\cdots,R_n)$,系统总的风险可通过求 $\boldsymbol{R}=f(w,\boldsymbol{R})$,$f(w,\boldsymbol{R})$为使用的综合评价函数,$w=(w_1,w_2,\cdots,w_n)^T$ 为风险的权重向量,$\boldsymbol{R}=(R_1,R_2,\cdots,R_n)^T$ 为系统风险向量,实现系统风险值的量化。

5 结束语

由于信息系统风险的不确定性,风险不易被准确量化。通过构建一种反映风险主要影响因素的多层综合评价指标体系,采用多级模糊综合评判法和熵权系数法对安全事件发生可能性及其产生影响进行多层量化评判,在一定程度上增强了评估结果的准确性和一致性。模糊综合评判法中对评价指标隶属度的确定,采用专家评判法,带有一定的主观性,对评估结果造成一定的影响。如何进一步减少评估中的主观性,使评估结果更客观准确是将来要研究解决的问题。

参考文献:

[1] 吴亚非,李新友,禄 凯.信息安全风险评估[M].北京:清华大学出版社,2007:9-10.

[2] 范 红,冯 国,吴亚非.信息安全风险评估方法与应用[M].北京:清华大学出版社,2006.

[3] 王英梅,王胜开,陈国顺,等.信息安全风险评估[M].北京:电子工业出版社,2007.

[4] Zhang Y R,Xian M,Wang G Y.A quantitative evaluation techunique of attack effect of computer network based on network entropy[J].Journal of Communications,2004,25(11):

(下转第 188 页)

DNS服务器用于将域名转换为其对应的 IP 地址。有了 DNS 服务,使用者就能通过在浏览器中输入域名来直接访问该系统,而不必输入该系统所在服务器的 IP 地址和访问端口号[7]。

系统发布时打包成为标准的 Windows Installer 安装程序包,可直接在安装包上双击执行。安装程序自动搜索并列出目标计算机 IIS 中可用的站点,在"Site"中选择将程序部署在哪个站点下,Virtual Directory 为虚拟目录名,在此指定为高校进修人员管理系统,单击下一步自动完成安装。

安装结束后,在 IIS 中找到"高校进修人员管理系统",右键点击"浏览"将出现系统默认的页面,部署工作完成(如图 4 所示)。

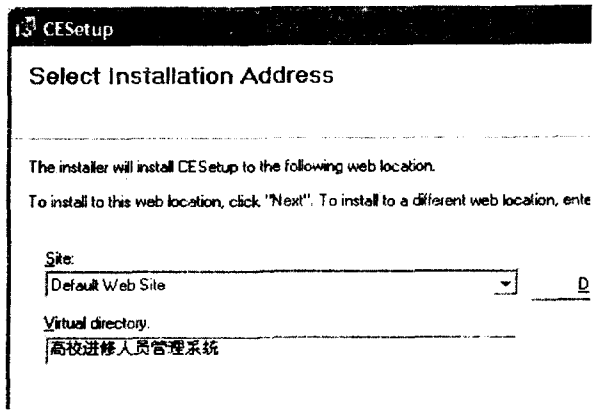

图 4 用 Windows Installer 安装本系统

除此之外,系统还可以通过 XCOPY 的方式将本站点所有内容直接拷贝到目标计算机 IIS 指定的虚拟目录下进行安装。

5 结束语

系统采用 B/S 架构模式设计,完全基于浏览器界面,安装方便,客户端只需安装普通的 IE 浏览器即可使用。CDM 不具体依附某一 DBMS,只是描述了数据库整体逻辑结构,通常包含了与具体物理数据库无关的数据对象,开发人员可以不受不同数据库管理系统实现上会有区别的影响,专心于数据库自身的设计中,通过 PDM 构建的数据库能充分发挥每种 DBMS 自身的特性。系统在安全上提供用户权限、密码验证并结合了操作系统、数据库的安全管理机制等各种安全策略,为系统正常运转提供安全保障。

参考文献:

[1] 魏宗秀.用 DIV 与 CSS 设计易于改版的 JKL 信息网页[J].淮北煤炭师范学院学报,2006,27(3):40-42.

[2] Jeffrey R. Applied Microsoft. NET Framework Programming [M]. US: Microsoft Press, 2002.

[3] 王 蕾,李培峰,杨季文.基于 ASP.NET 的 Web 应用系统架构探讨[J].计算机工程与设计,2006,16(7):55-58.

[4] Norman R J. Object - oriented Systems Analysis and Design [M].北京:清华大学出版社,2000.

[5] 陈 渝,秦开大,田 亮.基于 PowerDesigner 的信息系统数据建模建设[J].昆明理工大学学报:理工版,2004,29(1):45-47.

[6] 周晓锋.高校进修人员管理系统[D].芜湖:安徽工程科技学院,2007.

[7] 赵 玮,唐 亮,张结魁.基于.NET2.0 的旅行社管理信息系统的设计与实现[J].计算机技术与发展,2007,17(12):158-161.

(上接第 180 页)

158-165.

[5] 肖 龙,方 勇,戴忠坤.基于模糊神经网络的信息系统风分析[J].计算机应用研究,2006(5):137-139.

[6] 杨慧敏,付 萍.基于熵权的多级模糊综合评价的应用[J].华北电力大学学报,2005(5):105-106.

[7] Zhao D M, Zhang Y Q, Ma J F. Fuzzy risk assessment of Entropy-weight coefficient method applied in network security [J]. Computer Engineering, 2004, 30(18): 21-23.

[8] 陈 亮.信息系统安全风险评估模型研究[J].中国人民公安大学学报:自然科学版,2007(4):51-52.

[9] 梁保松,曹殿立.模糊数学及其应用[M].北京:科学出版社,2007:146-147.

(上接第 184 页)

[2] 屈晓辉.网络安全身份认证研究[M].北京:清华大学出版社,2006.

[3] 范林秀,陈舒娅,王喜进.基于 PKI 的身份认证在电子商务中的研究[J].电脑知识与技术,2007,16(9):979-980.

[4] 徐小平,尹颖禹.基于数字签名的身份认证模型的一种方案[J].计算机技术与发展,2006,16(2):121-123.

[5] 邢长明,刘方爱.基于 P2P 的网格资源发现机制研究[J].计算机技术与发展,2006,16(8):21-24.

[6] Isomura M, Decker C, Beigl M. Generic Communication Structure to Integrate Widely Distributed Wireless Sensor Nodes by P2P Technology [EB/OL]. 2006-04. http://www.teco.edu/michael/publication.

[7] Ripeanu M, Foster I, Iamnitchi A. Mapping the Gnutella network: Properties of large-scale peer-to-peer systems and implications for system design[J]. IEEE Internet Computing, 2002, 6(1): 50-57.