

基于改进身份认证协议的单点登录系统研究

马 蕾, 杨洪雪, 朱青松

(北京电子科技职业学院, 北京 100086)

摘 要: 研究基于改进身份认证协议的单点登录系统, 提高系统的身份认证的速度. 针对单点登录系统中进行身份认证时, 如果用户数据量过大, 导致用户需要逐个核对数据库中的身份信息, 造成的身份核对方法耗时, 延长了单点登录系统身份认证的时间. 为了避免上述问题, 提出了一种基于改进身份认证协议的单点登录系统. 利用线性回归方法, 对用户数据进行融合处理. 通过非线性传输参数方法将融合后的信息传输到服务器中, 并利用参数配准和身份认证技术将其与数据库中数据进行配准, 避免传统方法大规模比对带来的缺陷, 提高了身份认证的速度. 实验证明, 该方法能够提高身份认证的速度, 效果令人满意.

关键词: 身份认证; 单点登录; 数据融合; 参数配准

中图分类号: TP391

文献标识码: A

文章编号: 1000-7180(2012)07-0180-04

Based on Improved Identity Authentication Protocol Single Sign-on System Research

MA Lei, YANG Hong-xue, ZHU Qing-song

(Beijing Polytechnic, Beijing 100086, China)

Abstract: Study the identity authentication protocol based on improved single sign-on system, improve the identity authentication of the speed. For the single point login system identity authentication, the user data caused by large amount of identity check long time, leading to users need to check a database of one identity information, and extended the single point login system the identity authentication of the time. In order to avoid these problems, and puts forward a kind of identity authentication protocol based on improved single sign-on system. First, the linear regression function algorithm, the user data initialized processing. And by using nonlinear transfer function will user information transmission to the server, and registration algorithm using parameters with the database data registration, and get the identity authentication, improve the identity authentication of the speed. The experiment proves that system improve the speed of the identity authentication, and satisfactory results have been obtained.

Key words: identity authentication; single point register; data fusion; parameters registration

1 引言

单点登录系统的身份认证, 一直是单点登录系统相关领域研究的热点问题^[1]. 当前, 主流的单点登录系统身份认证方式主要包括基于数据融合的身份认证协议、基于 SPI 结构模型的身份认证协议、基于小波分解算法的身份认证协议和基于生物特征的身份认证协议等^[2]. 随着计算机技术的不断发展, 单点登录系统身份认证协议越来越受到重视.

这些传统算法在实际应用中, 会存在一个问题. 假设用户身份认证信息参数集合中的样本数目过大, 那么会造成与其对应的对比系数过大, 导致其绝对值对数变换函数值过大, 单点登录系统身份认证需要对所有参数依次进行对比分析, 最终导致需要计算的步骤过多, 耗费的时间过长. 因此, 缩短单点登录系统身份认证时间, 成为单点登录系统身份认证领域研究的一个难点问题^[3].

为了避免上述问题, 文中提出了一种改进的单

点登录系统身份认证方式. 首先,利用线性回归算法,对用户相关信息参数进行融合处理,为数据配准提供了数据基础^[4]. 其次,利用非线性传输方法,将融合处理后的数据传输到服务器中. 再次,利用细节点参数配准算法,将传输到服务器中的用户信息相关参数与数据库中信息进行配准^[5]. 最后,利用数字证书算法进行核对,提高单点登录系统身份认证的速度.

2 单点登录系统身份认证原理

单点登录系统身份认证协议,就是在登录时,利用智能方法及时迅速地对用户身份进行验证,保证用户身份的真实性^[6]. 其原理如下所述:

首先需要对用户身份相关信息进行相应的转换,选取合理的身份信息相关参数,然后利用公式(1),得到其傅立叶变换系数:

$$Y(l) = G[y(p)] = \sum_{p=1} y(p) \log(k+P)^2$$

$$= \sum_{p=P_1} y(p) \log(k+P)^2 \quad (1)$$

其中, $Y(l)$ 是身份认证用户相关信息傅立叶变换系数, $y(p)$ 是用户信息相关参数, P 是用户信息数据集合中的样本序号. 将根据公式(1)得到的结果,带入公式(2),获取其绝对值对数变换函数值:

$$D(l) = \log |Y(l)| \quad (2)$$

将根据公式(2)得到的变换结果,与用户信息数据集合中的用户参数进行对比分析. 假设数据集合中没有与其对应的用户参数,则用户认证失败,退出程序. 假设数据集合中存在与其对应的用户参数,则需要利用公式(3)对其进行傅立叶反变换:

$$d(p) = G[D(l)] = \sum_{l=1} D(l) \log(k/P) \quad (3)$$

将得到的结果发送到服务器中,则实现了用户身份认证. 为了衡量认证的实时性,利用公式(4)能够计算用户身份认证需要的时间:

$$t = \sum_{j=1} d(p)^2 (P-1)/k \quad (4)$$

通过以上原理可以推断,如果用户信息数据集合中的样本数量比较多,则公式(1)中 P 的取值比较大,则利用公式(1)得到的用户身份相关参数傅立叶变换系数偏大,那么根据公式(2)能够得知用户身份相关参数对数变换函数取值偏大,造成利用公式(3)得到的身份相关参数反傅立叶变换系数偏大,最终导致利用公式(4)分子变大,得到的身份认证时间过长,无法实现单点登录系统实时身份认证.

为了解决上述问题,提出了一种改进的单点登

录系统身份认证方式,首先对用户信息进行处理,然后将处理后的信息输入到服务器中,与服务器中信息进行配准. 假设配准成功,则利用数字证书对用户信息进行核对,从而提高身份认证的速度.

3 单点登录系统身份认证改进算法

利用单点登录系统身份认证算法,将用户参数信息与服务器中信息进行配准,从而实现单点登录系统快速身份认证. 其原理如下所述:

3.1 线性回归算法

假设用户信息系数集合是 $\{\sigma_j\}$,其中, j 是样本数量,那么可以利用公式(5)对用户进行线性分类:

$$z_j(x/y_j - c) > 1 \quad (5)$$

从而建立与用户对应的不同用户信息参数的映射,然后利用公式(6)对上述结果进行优化处理,从而获取最佳映射关系:

$$\max \lg \sum_{j=1} \sigma_j / P + \sum_{k=2} \sigma_j \sigma_k L(\sigma_j + \sigma_k)^2 \geq 1 \quad (6)$$

再利用公式(7)建立与其对应的线性回归函数:

$$L(y_j, z_j) = \varphi(y_j) / \varphi(z_j) \quad (7)$$

其中, $\varphi(y_j)$ 是需要输入的用户个人信息系数分量到服务器中的映射, d 是有一定取值范围的常数,用于调整数据偏差, b_j 是Lagrange参数. 假设 b_j 的取值是非零整数,则输入的用户相关信息系数用 t_j 表示,从而能够利用公式(8)获取决策函数:

$$g(y) = \sum_{j=2} b_j z_j / L(t_j) - c \quad (8)$$

其中, c 是用户相关信息参数数据偏差,利用线性回归函数,能够将非线性的用户相关信息数据分类映射到服务器中.

所有的用户相关信息参数分量都拥有与其对应的规则,针对所有的用户相关信息参数系数 σ_j ,设置 $D_{j,j}$ 是与其对应的 σ_j 隶属度函数极大值模糊数据集合,那么能够得到与其对应的规则集合 $\{jD_{j,1}, jD_{j,2}, \dots, jD_{j,l}\}$.

将用户相关信息参数系数和对应的规则利用临近区域权值系数融合算法进行特征级别融合处理,设置用户相关信息参数数据集合中样本数量是 P ,样本类别是 D ,那么利用临近区域权值系数融合算法进行特征级别融合处理的具体步骤如下所述:

(1) 通过邻近区域类别管理器获取每个类别样本中的数据与服务器中数据的相似性;

(2) 将获取的样本相似性系数按照逐个递增方式进行排序($e_1 < e_2 < \dots < e_n$),从而获取相似性极小值 e_1 ;

(3) 利用公式(9)计算用户相关信息参数相似性系数:

$$\bar{e} = \sum_{j=1} e_j / d \quad (9)$$

(4) 样本相似性系数均值与相似性系数极小值之比用公式(10)计算:

$$u = \bar{d} / d_1 \quad (10)$$

(5) 用户相关信息参数系数与服务器中对应数据的比值用公式(11)计算:

$$x_j = \sigma_j / \sigma'_j \quad (11)$$

(6) 计算用户相关信息参数样本权值系数 $x = [x_1, x_2, \dots, x_n]$, 利用公式(12)获取权值系数平均值 $\bar{x}$:

$$\bar{x} = (\sum_{k=1} x_k / N) \quad (12)$$

(7) 最终获取临近区域权值系数融合公式:

$$z = [\sigma_j, \bar{x}, z_j] \quad (13)$$

通过上述步骤能够将身份认证参数进行融合处理, 为提高身份认证的速度提供了数据基础。

3.2 参数配准

利用非线性传输方法, 能够将用户信息传输到服务器中, 将其与服务器中数据进行对比, 是身份认证中使用的数据传输方式, 其原理如下所述:

假设用户相关信息参数是利用高斯函数进行变换处理的, 那么与其对应的第 j 个待传输用户数据利用公式(14)能够得到:

$$A_j(u) = L(|\sigma_k(u) - T_j|) \\ = \lg \left[\sum_{k=2} (\sigma_k(u) - T_j)^2 / b_j^2 \right] \quad (14)$$

其中, $A_j(u)$ 是第 j 个待传输用户信息, $\sigma_k(u)$ 是第 j 个用户相关信息参数, T_j 是第 j 个用户信息变换矢量, b_j 是对应的传输控制系数。

用户身份信息参数的关键细节特点存在一定程度的偏差, 而且这些关键细节特点保持一定的状态不发生改变。假设对其进行数据配准, 那么可以提高单点登录系统身份认证的抗干扰能力, 避免利用复杂的计算对用户身份信息参数进行预处理, 减少单点登录系统身份认证的步骤, 从而提高身份认证的速度。其原理如下所述:

(1) 将所有用户身份认证参数建立数据集合:

$$A_j = \{A_{jk}\}_{k=2}^{D_j} \quad (15)$$

其中, A_{jk} 是身份认证参数系数。

(2) 对身份认证参数系数数据集合中的样本利用小波变换算法进行解析, 从而获取其小波变换关键细节特点数据集合:

$$X_j = \{X_{jk}\}_{k=2}^{D_j}, k=2, 3, \dots, D_j \quad (16)$$

(3) 将身份认证参数系数及其小波变换关键细节特点进行数据配准, 得到数据集合:

$$G_j = \{G_{jk}\}_{k=2}^{D_j} \quad (17)$$

(4) 利用公式(18)能够计算邻近区域用户参数关键细节特点相关性系数取值:

$$\sigma_k = D(G_{jk} + G_{jk-1})^2 / \sqrt{E(G_{jk}) \cdot E(G_{jk-1})} \quad (18)$$

其中, $E(G_{jk})$ 是 G_{jk} 的方差, $D(G_{jk} + G_{jk-1})^2$ 是 G_{jk} 和 G_{jk-1} 的均值平方和。

(5) 利用公式(19)能够得到用户参数信息系数均值:

$$\sigma_{ave} = \sum_{k=2} \sigma_k(p) / (D_j + 1) \quad (19)$$

(6) 利用公式(20)能够计算临近区域用户身份信息参数相关性系数衡量标准:

$$\sigma = u \cdot \sigma_{ave} \quad (20)$$

其中, u 是具有一定取值范围的常数, 能够按照实际情况对身份认证相关信息参数进行调整, σ 是邻近区域用户身份信息参数相关性系数衡量标准。

(7) 将所有的用户相关信息参数与数据库中信息进行相关性系数计算, 从而获取相邻区域用户参数信息相关性系数极大值 $\sigma_{max} = \max\{\sigma(j)\}$ 。其中, j 是用户在数据集合中的序号。

(8) 假设根据步骤(7)得到的结果大于邻近区域用户信息参数相关性系数极大值, 那么确定该用户是数据库中序号是 j 的用户, 否则, 确定该用户是非法用户, 退出程序。

通过上面阐述的方式, 能够及时进行单点登录系统的身份认证, 提高了单点登录系统身份认证的速度。

3.3 数字证书身份信息核对

利用数字证书身份认证方式能够进行单点登录身份信息核对, 应该首先将用户相关信息发送到服务器中, 然后获取该用户的数字证书。这个数字证书能够用于单点登录系统用户身份认证, 从而有利于提高用户身份认证的速度。

首先, 用户需要利用浏览器向需要登录的服务器提出登录申请; 其次, 服务器会发送信息, 要求用户发送自己的数字证书; 再次, 用户发送自己的数字证书到服务器中; 最后, 服务器将用户发送的数字证书相关信息在服务器中进行核对, 确认该用户信息的真实性; 利用上面阐述的数字证书身份认证方式, 能够提高单点登录系统身份认证的速度。

4 实验结果及分析

为了验证本文提出的基于改进身份认证协议的单点登录系统方式的有效性,需要进行一次实验,其步骤如图 1 所示。

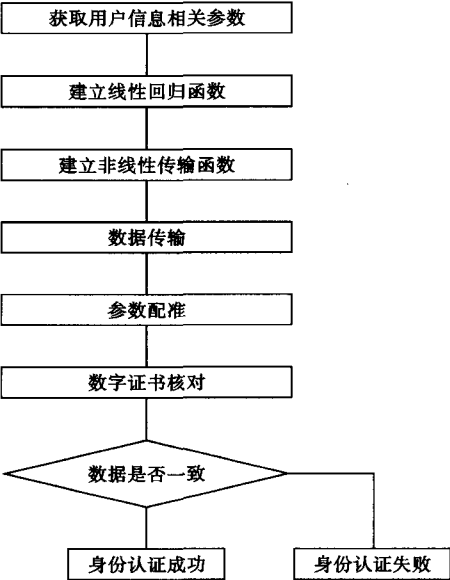


图 1 身份认证流程图

分别用传统算法和本文算法进行单点登录系统的身份认证. 设置系统数据库中样本数量是 1000, 则单点登录系统身份认证耗费时间如图 2 所示。

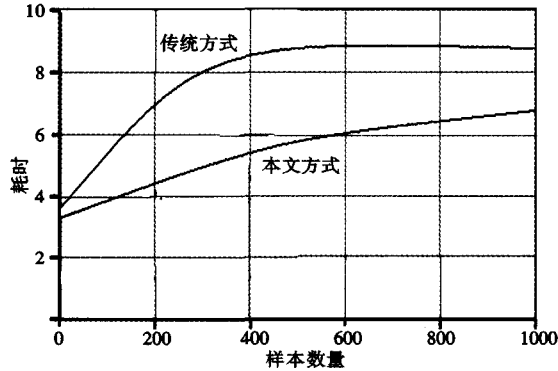


图 2 不同方式进行身份认证耗费时间

可以看出,在用户相关参数数据集合中样本数目比较多时,利用本文方式进行身份认证耗费的时间比传统方式短很多. 在实验过程中,利用公式(4)能够计算单点登录系统用户身份认证耗费的时间,其相关数据用表 1 描述。

通过表 1 得知,利用传统方式进行单点登录系

统身份认证,需要将用户输入的信息与服务器中对应的数据库中信息依次进行对比分析,耗费的时间大于本文方式。

表 1 不同方式身份认证耗费时间表

	样本数量/个	时间/s
本文方式	1000	9
传统方式	1000	7

5 结束语

文中提出了一种基于改进身份认证协议的单点登录系统. 建立用户相关信息参数线性回归函数,将数据进行融合处理,并且将处理结果进行配准,从而实现快速的单点登录系统身份认证. 随着各种应用系统对用户信息核对的需要越来越高,本文的研究具有较高的实用价值。

参考文献:

[1] 师黎,朱民杰. 基于遗传算法优化 BP 神经网络在心电图身份识别中的应用[J]. 中国组织工程研究与临床康复,2010(43):8069-8072.

[2] Wilson CL, Candela GT, Watson Cl. Neural network and fingerprint classification[J]. Artific Neural Networks,2003;45-50.

[3] 杨向林,严洪,李延军,等. 基于小波分解和数据融合方法的 ECG 身份识别[J]. 航天医学与医学工程,2009,22(4):296-301.

[4] 孙冬梅,裘正定. 生物特征识别技术总述[J]. 电子学报,2001(29):27-32.

[5] 万励,吴洁明. P2P 网络环境下一种快速身份认证策略的研究[J]. 计算机仿真,2011(8):141-145.

[6] 向元平,宁子岚. 基于人脸识别的双因素身份认证系统的设计与实现[J]. 计算机测量与控制,2009(5):959-961.

作者简介:

马 蕾 女,(1979—),硕士,讲师. 研究方向为中国农业大学 计算机科学、计算机应用。

杨洪雪 女,(1972—),硕士,副教授. 研究方向为计算机科学与应用、职业教育学。

朱青松 男,(1973—),博士. 研究方向为语言识别与智能机器人。