

统一身份认证技术在高校数字化校园中的应用

田永晔 王晶晶

(扬州市职业大学 信息工程学院, 江苏 扬州 225000)

摘要: 常规的高校数字化校园身份认证技术利用最低有效位生成隐藏矩阵, 需要多用户完成, 导致其信息隐藏容量不足, 因此需要提出一个新的高校数字化校园身份认证技术。先建立统一身份数据库, 根据数据库设定身份认证目标逻辑指令, 再构建循环认证模式, 最后生成高校数字化校园身份认证。实验结果表明, 设计的高校数字化校园身份认证技术安全性较高, 认证效果较好, 可以有效地抵御众多已知的安全威胁, 具有一定的应用价值。

关键词: 统一身份认证技术; 高校数字化校园; 数据库

中图分类号: TH164 **文献标识码:** A **文章编号:** 1003-9767 (2024) 05-236-003

The Application of Unified Identity Authentication Technology in the Digital Campus of Colleges and Universities

TIAN Yongye, WANG Jingjing

(School of Information Engineering, Yangzhou Polytechnic College, Yangzhou Jiangsu 225000, China)

Abstract: The conventional digital campus identity authentication technology of colleges and universities uses the lowest effective bit to generate the hidden matrix, which needs to be completed by multiple users, resulting in insufficient information hidden capacity, so it is necessary to propose a new university digital campus identity authentication technology. First, a unified identity database is established, and the logical instruction of the identity authentication target is set according to the database. Next, the circular authentication mode is constructed. Finally, the digital campus identity authentication is generated. The experimental results show that the digital campus identity authentication technology designed by universities is highly secure, the authentication effect of the technology is good, which can effectively resist many known security threats, has certain application value.

Keywords: unified identity authentication technology; university digital campus; database

0 引言

随着信息技术的不断发展和各高校数字化建设的不断深入, 统一身份认证技术在高校数字化校园中的应用使得跨多个系统的无缝访问成为可能, 为数字化校园建设的安全性和可靠性提供了有力保障。在高校数字化校园建设中, 统一身份认证技术的作用主要体现在以下方面。首先, 能够实现用户身份的集中管理和保护, 确保

用户数据的保密性和完整性。其次, 可以实现单点登录, 即用户只需要使用一个账号和密码就可以访问多个系统^[1]。最后, 可以对用户权限进行精细化管理, 实现对不同用户访问不同资源的控制, 有效防止数据泄露和滥用。未来, 将统一身份认证技术与物联网、人工智能等先进技术相结合, 进一步拓展其在智能管理、安全监控等方面的应用。

收稿日期: 2024-01-11

基金项目: 江苏省现代教育技术研究 2018 年度课题“基于数据共享和统一身份认证机制的高校数字化校园应用系统集成方案研究”(项目编号: 2018-R-66272)。

作者简介: 田永晔(1976—), 女, 江苏泰兴人, 本科, 讲师。研究方向: 计算机应用技术。

1 高校数字化校园身份认证技术设计

1.1 建立统一身份数据库

统一身份数据库的建设步骤如下：一是收集和整理人员信息，如身份证号、性别等，并将其存储在可靠的数据库中；二是对部分账号进行唯一的关联，如将人员的编号与账号进行关联，以确保账号的唯一性和准确性；三是每个人使用不同的人员编号，以确保人员信息的唯一性和准确性；四是及时更新账号信息，以确保数据的准确性和一致性^[2]。

1.2 设定身份认证目标逻辑指令

根据目标的不同阶段性结构进行层次分级，在符合逻辑目的的前提下，设置身份验证过程^[3]。该方法首先要确定逻辑验证的范围，然后计算平均逻辑指令，计算公式为

$$N = \varepsilon + \frac{R}{3} + 3\delta \quad (1)$$

式中： N 表示平均逻辑指令； ε 表示张力间距； R 表示验证距离； δ 表示容许的限制误差。通过计算得到平均的逻辑指令。在整个逻辑结构中设置适当的审计协议，协议的功能是二次验证用户的身份。设置二次验证的原因是环境的改变和调整经常会导致协议指令产生错误，给平台的操作带来更大的难度和阻力。在这种情形下，辅助验证能最大限度地保证用户身份识别的准确性。根据所设置的指示和请求，将目标逻辑结构放入下一步的确认过程中，确定最初的指令，并计算多点逻辑目标确认系数，计算公式为

$$K = \sqrt{2N + 1.5} - 3\theta + \frac{1}{2} \quad (2)$$

式中： K 表示多点逻辑目标确认系数； N 表示平均逻辑指令； θ 表示多点错误值。计算得到多点逻辑目标确认系数，将实际测量准则相对应的目标确认因子与用户标识一起进行验证。基于以上测量条件，完成验证逻辑指令的设置。

1.3 构建循环认证模式

根据设定的身份认证目标逻辑指令，构建循环认证模式。图1为循环认证流程图^[4]。

循环认证具体步骤如下：步骤一，用户向认证服务器发送身份认证请求，提供身份信息，如用户名、密码等；步骤二，认证服务器接收用户请求，并进行初次身份验证，如果初次验证失败，则向用户发送挑战信息，如随

机数或加密的挑战字符串；步骤三，用户根据挑战信息进行响应，并将响应结果发送给认证服务器；步骤四，认证服务器对响应结果进行验证，并根据验证结果决定是否授予访问权限。如果验证失败，则重新发送挑战信息，并重复步骤三和步骤四，直到达到预设的认证次数限制或者成功通过认证；如果认证成功，则用户获得访问权限，可以进行相关操作。

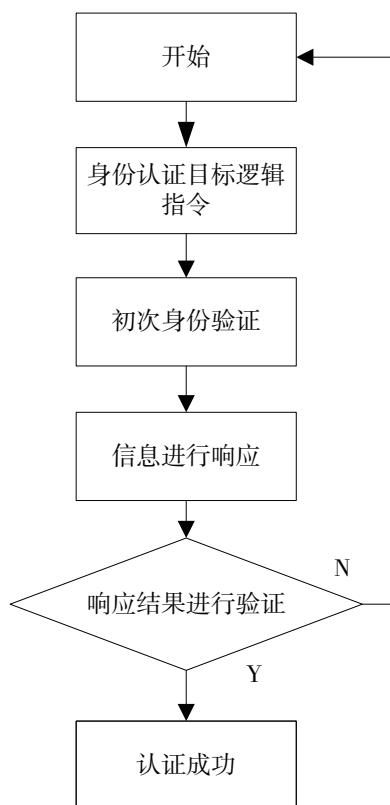


图1 循环认证流程图

1.4 生成高校数字化校园身份认证

针对上述构建循环认证模式，可以建立合理的连接认证子模块。首先，需要将认证接口插入认证终端，进行初次身份认证识别，发送此时得到的认证请求消息。其次，由云服务器确定响应请求的响应效果，并提取相关的验证信息，若此时认证通过，则会由管理员向虚拟机队列发送有效的查询信息，反之需要重新确定虚拟空间的使用率，得到全新的任务参数，进行二次任务反馈。最后，从各个反馈中挑选符合认证需求的指令，与云服务器终端建立有效连接，从而提高认证的安全性，保证认证服务可以被实时中断。根据上述内容生成高校数字化校园身份认证协议^[5]。

2 实验论证分析

为了验证上文设计的高校数字化校园身份认证技术

的实际认证效果，将 IPv6 身份认证技术和二维码身份认证技术设置为对照，开展校园身份认证实验，具体过程如下。

2.1 实验准备

实验平台选用了 OPNET。在实验环境方面，选择了 Windows 7 操作系统，并配备了主频为 3.2 GHz 的中央处理器，以满足大多数网络应用需求，并能够保证实验的可靠性和准确性。

2.2 实验结果分析

实验结果如表 1 所示。由表 1 可知，IPv6 身份认证技术未提供智能卡撤销操作，这无疑是一种在安全性上

的缺陷，无法有效抵御隐藏服务器攻击。而且，IPv6 身份认证技术包含大量的指数运算，在一定程度上增加了计算的开销。二维码身份认证技术具有固有的局限性，使得其无法抵御在线密码猜测攻击、隐藏服务器攻击等攻击手段。文章所提技术在满足众多安全要求的同时，可以有效地抵御众多已知的安全威胁。因此，该身份认证技术具有一定的应用价值，可以为高校数字化校园的安全性和可靠性提供有力的保障。通过使用该技术，高校可以有效地提高数字化校园的安全性和可靠性，保障用户信息的保密性和完整性，为用户提供更加便捷和安全的数字化校园环境。

表 1 不同技术安全性的对比结果

安全特征	IPv6 身份认证技术	二维码身份认证技术	文章所提技术
提供双向身份认证	✓	✓	✓
抵御恶意用户攻击	✓	✓	✓
提供前向保密性	✓	✓	✓
具备用户匿名性	✓	✓	✓
抵御重放攻击	✓	✓	✓
抵御在线密码猜测攻击	×	×	✓
抵御内部攻击者	✓	×	✓
提供智能卡撤销功能	×	✓	✓
抵御隐藏服务器攻击	×	×	✓

3 结语

采用统一身份认证技术，高校能够有效地提高数字化校园的安全性和可靠性。师生只需要使用一个账号和密码就能够跨多个系统进行无缝访问，不仅减少了管理成本，而且大大提高了工作效率。此外，该技术能够实现对用户权限的精细化管理，确保不同用户只能访问其所需的数据和资源，有效避免了数据泄露和滥用。在未来，随着数字化校园的不断发展和完善，统一身份认证技术的应用场景将会更多。

参考文献

[1] 庄仁峰,黄伟湘,黄健文,等.移动认证:基于运营

商通信网络的统一身份认证技术[J].网络空间安全,2022,13(6):63-68.
[2] 吕忠亭,崔巍,刘洋,等.高职院校智慧校园统一身份认证技术分析[J].计算机与网络,2020,46(21):69-72.
[3] 廖会敏,俞果,班国民,等.基于国密 SM9 算法的电力物联网身份认证技术研究[J].山东电力技术,2020,47(10):1-5.
[4] 周启扬,李飞,章嘉彦,等.基于区块链技术的车联网匿名身份认证技术研究[J].汽车技术,2020(10):58-62.
[5] 邱帆,胡凯雨,左黎明,等.基于国密 SM9 的配电网分布式控制身份认证技术[J].计算机应用与软件,2020,37(9):291-295.