



基于指纹识别的云安全认证技术

汤雅妃,张云勇,张 尼

(中国联合网络通信有限公司研究院 北京 100032)

摘 要:在云计算环境中,作为云安全的第一道防线,用户身份认证有着至关重要的作用。分析了当前云服务系统的认证需求,考虑到指纹识别技术在云安全认证中的应用优势,提出了一种基于指纹识别的云安全认证系统。并对其系统架构、工作流程进行了深入研究,以通过更加安全的认证方式防止恶意用户的非法访问,保证云环境下用户数据的访问安全。

关键词:云计算;云安全;指纹识别;身份认证

doi: 10.11959/j.issn.1000-0801.2015211

Cloud Security Certification Technology Based on Fingerprint Recognition

Tang Yafei, Zhang Yunyong, Zhang Ni

(China Unicom Research Institute, Beijing 100032, China)

Abstract: As the guarantee of cloud security, user identity authentication is crucial to cloud computing. In this work, the requirements of security authentication in the current cloud service systems were analyzed. Considering the principle and the advantages of fingerprint recognition, a novel system based on fingerprint recognition was proposed for cloud security authentication. The architecture and workflow of the proposed system were investigated in depth to prevent the unauthorized access, achieving the secure access of user data for cloud services.

Key words: cloud computing, cloud security, fingerprint recognition, identity authentication

1 引言

云计算作为一种新的计算方式和商业模式,通过互联网为用户提供动态部署、按需分配的计算、存储、软件、平台等资源服务^[1],并实时监控资源使用情况。作为当前发展最为迅速的新兴产业之一,云计算具有广阔的市场前景,同时也面临着前所未有的安全挑战。据调查显示,云安全不仅成为用户使用云服务的最大顾虑,也是云应用广泛推

广的首要障碍之一。

云服务系统由于需要对用户进行远程身份认证,因此对认证系统的安全性要求更高。本文设计的云安全认证系统基于三层 B/S 结构,采用分布式网络技术,将海量指纹信息根据地域和用户级别进行分布式分类存储。进行身份认证时,首先采用双向认证机制建立客户端与云端服务器的安全信道,确保认证过程的安全进行,防止指纹密钥和传输数据被窃取。然后通过指纹识别技术对采集到的指纹

收稿日期:2015-07-23;修回日期:2015-08-06

论文引用格式:汤雅妃,张云勇,张尼. 基于指纹识别的云安全认证技术.电信科学,2015211

Tang Y F, Zhang Y Y, Zhang N. Cloud security certification technology based on fingerprint recognition. Telecommunications Science, 2015211

信息依次进行特征提取、加密封装、信道传输、解密还原、特征匹配,从而确定用户身份,控制用户访问权限。

2 云安全认证

2.1 云安全认证需求

在云计算模式中,由于用户的数据和计算并非本地存储,而是交付到云端服务器保存、运行以及共享资源,因此需要为用户提供一个高信任度的安全访问机制。除了关注云端数据的可靠性与稳定性,更应当保证用户端与云端的安全接入。用户能否安全登录云端是云计算应当首要解决的安全问题,否则基于云端的一切服务都将变得不可信,难以得到用户的认可^[1]。

据调查,近几年发生的数据泄露事故有 70%以上都是通过外部的访问源进入系统的。2013 年 12 月,我国电商领域爆发用户泄露事件,泄露总量达 2 500 万。2014 年 9 月,苹果 iCloud“艳照门”事件爆发,黑客暴力破解 iCloud 用户设置的弱口令入侵账户,101 位美国好莱坞女星私密照片被公布于互联网。可见,用户是整个云服务系统中不可缺少的因素,同时也是安全性最为薄弱的部分。为了保证云服务的安全,必须对进入系统的用户进行有效身份认证,根据识别出的用户身份与授权数据库匹配,从而决定用户能否有权访问资源。

2.2 云安全认证方式

用户在进入系统或访问不同保护级别的系统资源时,系统需要通过一定的认证手段来验证被认证对象属性以确认其是否真实有效且唯一^[2]。基于认证对象属性,目前移动终端的认证方式主要包括口令认证、智能卡认证、数字证书以及生物特征认证。

2.2.1 口令认证

口令认证是最常见也是最简单的云安全认证技术之一,主要表现形式有静态口令、动态口令以及 PIN 码。认证系统记录每个用户的身份 ID 和对应的通行口令,当用户

访问云端时通过判断用户提供的 ID 和口令是否有效决定用户访问权限。该方式简单易用,然而容易遭受口令猜测和截获攻击,只能实现对用户端单向认证,不能防止云端服务器的假冒攻击。

2.2.2 智能卡认证

智能卡在身份认证中起了通行令牌的作用,可存储安全控制软件及用户的个人数据,用户登录时必须将其插入专用的读卡器读取信息以验证用户身份。相对于口令认证,智能卡不仅能够安全存储密钥、口令等机密信息,还可以内置加解密算法,存储私有密钥、数字证书、生物特征等用户独有信息,使得身份识别更安全、保密程度更高。但是由于智能卡必须配合读卡器才能完成操作,因而容易损坏、丢失和被盗,有一定的硬件支出和地域限制^[3]。

2.2.3 数字证书

数字证书是用户的电子身份标识,由认证服务器利用用户公钥解密,并检验数据完整性以确认签名的合法性,是目前公认的网络中最为安全有效的身份认证手段之一,也是云安全认证的最主要方式。用户使用数字证书可以保证信息传输中的保密性、完整性、身份的真实性以及交易的不可抵赖性。然而该认证方式需要对证书进行请求、发送和校对等操作,降低了通信效率,增加了服务器的计算负担,限制了应用扩展性^[4]。

2.2.4 生物特征认证

生物特征认证采用人的生理特征或行为特征作为认证手段,是目前正在迅速普及的一类新兴认证方式。认证系统首先从用户生物特征库中提取唯一标识的特征模板并进行数字化处理,并将这些模板存储在识别系统的数据库中。进行身份认证时,认证系统再将当前采集到的生物特征与存储模板进行匹配以确定用户身份。从理论上说,生物特征认证具有唯一性、永久性、普遍性、便携性,安全性更高且用户体验更好。现阶段的生物认证方式主要包括指纹、虹膜、人脸、声音、笔迹等,其性能见表 1。

表 1 生物特征识别技术性能比较

类型	可靠性	稳定性	接受性	唯一性	采集性	防伪性	普遍性
指纹	高	高	高	高	中	中	高
虹膜	高	高	低	高	中	高	高
人脸	低	中	高	低	高	低	高
声音	中	低	高	低	中	低	中
笔迹	中	低	高	低	中	低	低



由表1可知,在现有生物识别技术中,指纹识别占据较大优势,将有助于提高云服务系统的用户接入安全保障。

3 指纹识别

3.1 指纹识别在云安全认证中的应用

指纹是指手指末端凸凹不平的纹路,这些纹路在图案、端点和交叉点上各不相同,称为指纹特征^[5]。指纹识别技术通过分析指纹的局部特征,从中提取出特征值,与指纹的特征模板进行匹配,从而可靠地确认用户身份。基于指纹识别的云安全认证技术具有以下优势。

- 唯一性:根据指纹学理论,世界上并不存在完全相同的两枚指纹。并且指纹特征不会丢失、不会遗忘、不易仿冒。指纹的唯一性为其用于身份鉴定提供了客观根据。
- 不变性:从总体上看,从人出生之日起,尽管随着年龄的增长,同一手指的指纹脊纹类型、细节特征的总体布局等始终无明显差异^[6]。
- 在云服务系统中,所有认证用户都是异地分布的,因而需要进行远程认证。由于指纹识别只需存储指纹图像的特征值,大大减轻了网络传输的负担以及系统模板库的存储量,便于实现指纹异地匹配。
- 现阶段指纹识别算法已经相当成熟,识别率越来越高。采用SSL技术、加密技术能够有效防止黑客截取用户信息,保证数据在网络上的安全传输。
- 指纹的采集相对容易,当前市场上已研发出多种类型的指纹采集设备。随着移动终端传感技术的发展,目前已可由手机、iPad等便携式移动终端实现指纹采集和处理工作。

与传统的认证方式相比,指纹作为人体独一无二的特征,不仅其复杂度可以提供用于鉴别的足够特征,还具备不易丢失、遗忘和伪造等天然优势,因而具有更高的可靠

性、安全性和有效性。同时随着信息技术的发展,指纹识别技术日趋成熟,作为网络和信息服务领域的一种新兴认证方式,基于指纹识别的云服务系统具有广阔的市场前景。

3.2 指纹识别原理

指纹识别系统(fingerprint identification system, FIS)的本质是模式识别,如图1所示,一个典型的FIS包括离线存储和在线识别两个阶段,涉及指纹采集、图像处理、特征值提取、指纹匹配4个步骤^[7],并由指纹数据库存储指纹特征模板。具体流程如下。

(1) 指纹入库

目的是获取用户注册样本、提取指纹特征值以生成指纹特征模板并入库存储。FIS首先对注册人员进行指纹采集,获得数字指纹图像矩阵;然后对得到的指纹图像进行还原、增强及细化处理,得到黑白二值图像;在此基础上,提取指纹特征值并与用户身份信息一起存入指纹数据库。

(2) 指纹识别

主要任务是在线实时采集待识别的指纹图像并提取特征值,通过指纹匹配算法对数据库中存储的指纹特征进行匹配,继而基于模糊理论计算相似度。待完成与数据库中所有指纹特征模板的匹配检索后,可以确认用户身份的合法性和访问权限。这一阶段的关键是指纹匹配算法的建立与实现,目前现有的模式识别算法基本上可以满足指纹识别的需要^[8]。指纹识别系统原理如图1所示。

4 基于指纹识别的云安全认证系统

4.1 系统架构

本文采用分布式服务架构设计了一个基于指纹识别的云安全认证系统,如图2所示。本系统的设计采用三层B/S架构,包括顶层客户服务端、中间层应用服务层以及底层数据库服务层。客户端负责用户指纹的采集和特征值提

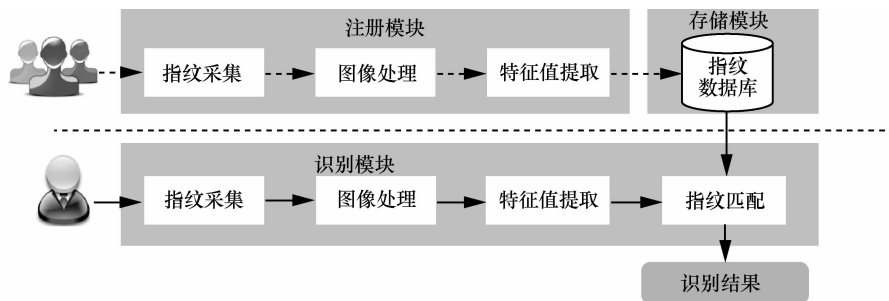


图1 指纹识别系统原理

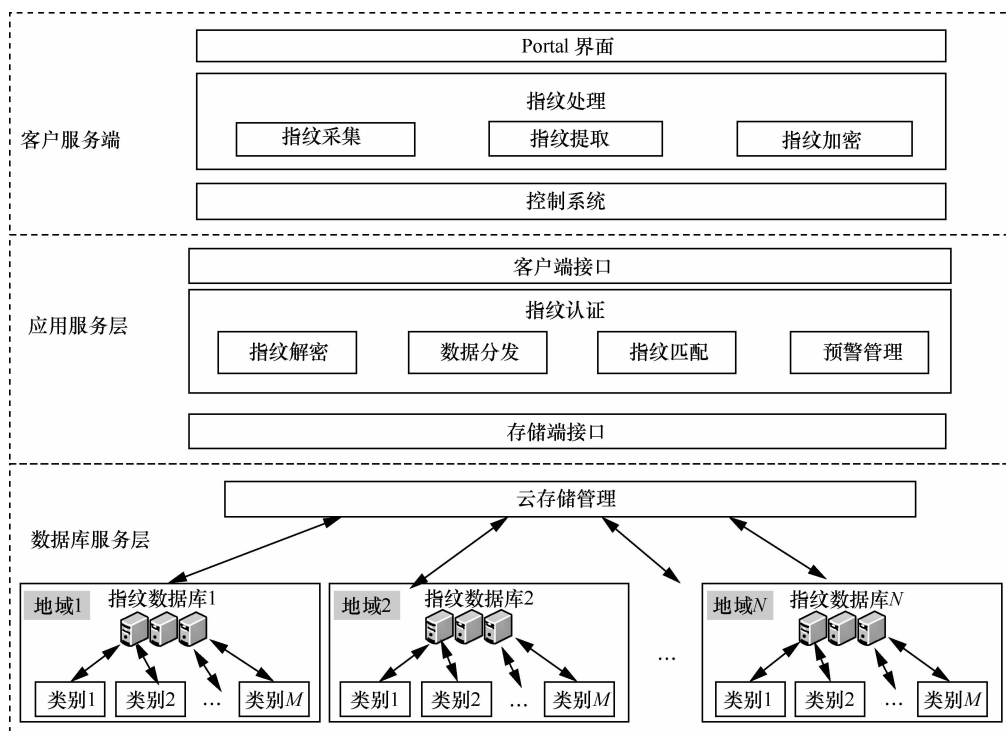


图 2 指纹识别认证系统架构

取,中间层由云端服务器完成指纹匹配,底层按照用户类别对指纹特征模板进行数据库分类存储。各层独立开发,各司其职,易于维护与管理,又减轻了服务器的处理负担,提高了系统的认证效率。

(1) 客户服务端

包括 Portal 登录界面、指纹处理系统以及控制系统。用户可登录 Portal 界面进行可视化认证操作。随着传感技术的发展以及内核操作系统的升级,当前用户终端(包括个人电脑和移动终端)不仅兼具了图像采集、特征值提取和信息加密等指纹处理功能,还具备对处理过程的全流程控制。

(2) 应用服务层

包括指纹认证模块以及面向客户端和用户端的交互接口。其中,指纹认证模块是整个认证服务系统的核心,包括指纹解密、数据分发、指纹匹配以及预警管理 4 个单元。云端服务器首先响应用户发来的服务请求,获取用户加密信息。然后通过解密算法还原用户信息(包括用户 ID)和指纹特征值。继而转发给相应地域下指纹数据库进行分类存储或者根据用户 ID 从对应的指纹数据库中提取出用户指纹特征模板进行指纹匹配,并将认证结果反馈给顶层客户服务端。如果用户发送的指纹特征值与数据库中存储的指纹特征模板匹配成功,则允许用户权限内操作,否则拒绝

用户登录。如果在认证过程中出现连续多次登录失败等异常操作现象,将由预警管理单元进行备案并通知系统维护人员。

(3) 数据库服务层

本系统采用分布式网络技术将海量指纹特征数据分布存储于不同地域下的指纹数据库中。云存储管理单元负责响应上层应用服务层的数据访问请求,指纹数据库用于数据的定义、访问、维护、更新和管理。为了提高认证效率,指纹数据库将按照用户级别进行分类存储,不同级别的用户对应不同的访问权限。

4.2 工作流程

在本文设计的云安全认证采用双向认证机制以提高系统的安全性。在进行指纹识别身份认证时,先采用加密协议使得客户端与云端握手成功,双向验证各自合法性后建立安全链接并获取共享密钥^[9]。接下来根据用户业务需求,进行用户指纹注册和指纹登录认证。

4.2.1 用户注册

每一个客户端要登录云端都必须先经过指纹登录注册,将自己指纹特征值和个人信息使用公钥进行加密再传给云端。云端服务器再使用自己的私有密钥解密用户注册密文,将用户信息存储入库^[2]。具体流程如图 3 所示。

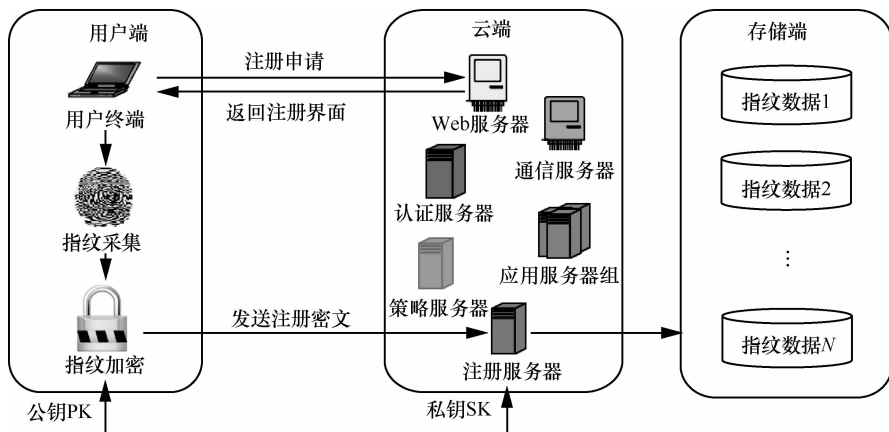


图3 用户指纹注册流程

当客户端向云端发送注册申请时,用户首先通过PC或者智能终端申请注册,Web服务器响应并反馈注册页面,用户端填写个人基本信息并通过指纹识别终端采集用户指纹,经指纹算法模块处理提取出指纹特征值。为了防止手指受伤等特殊情况,可以输入多个指纹并进行多次采集。接下来用户将个人信息(包括用户ID、用户权限等)、采集到的指纹特征模板、认证时限和现时数据经公钥加密后发送给云端注册服务器。服务器接收到用户的注册密文后,使用自己的私钥进行解密,并将用户的指纹特征模板和个人信息按照固定格式封装成一条用户注册记录发送给相应地域的指纹数据库进行分类存储,每条注册记录对应一个用户ID,用于用户下次登录时进行指纹认证。

4.2.2 登录认证

用户访问云端需要进行登录认证,将采集到的用户信

息与指纹模板以及认证时限等参数加密后发送至云端,由云端服务器进行解密还原用户ID和指纹特征值,从指纹数据库中搜索出用户ID对应的注册记录与指纹特征值进行匹配。具体流程如图4所示。

用户访问云端时首先登录Portal界面提交登录申请,Web服务器响应申请请求并建立安全通道。利用用户终端的指纹传感器,如RFID卡等,完成指纹采集,提取出指纹特征,再将用户的ID、指纹特征以及认证时限和现时数据用公钥加密后生成认证密文发送给云端的认证服务器。当认证服务器接收到当前用户的认证密文后,首先使用自己的私有密钥进行解密,还原出用户认证信息,并根据用户ID查找对应的指纹数据库。若该数据库中并不存在此用户ID,则用户无效,返回认证结果并退出认证系统;若存在,则返回该用户ID对应的注册记录并提取出该记录中的指纹特征模板。接下来认证服务器将当前用户指纹特征

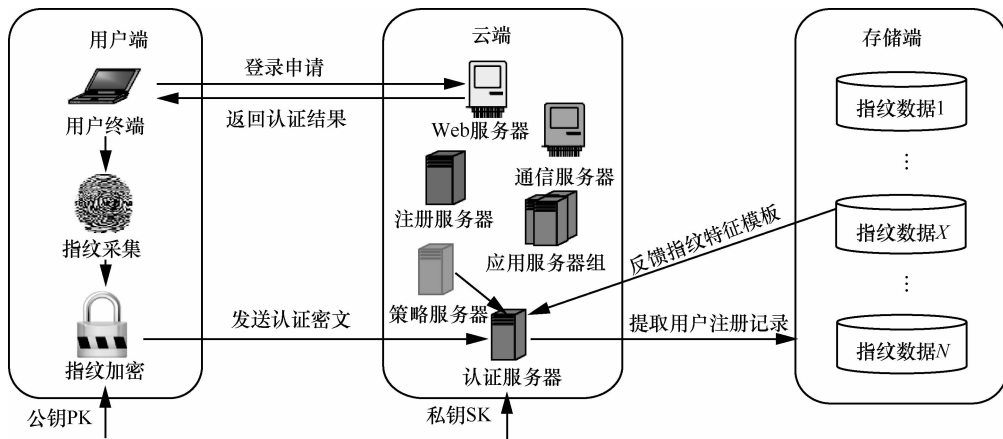


图4 用户指纹认证流程

值与用户ID对应的指纹特征模板进行匹配,从而判断用户身份。若匹配失败,此次认证无效,开始新一轮认证;若成功,认为用户身份合法,然后根据用户ID查询策略服务器得到用户权限。用户端可以与云端进行通信,基于用户权限访问相应的云服务。

为了提高认证系统的安全级别,在认证过程中可以设置认证阈值,当用户认证次数超过该阈值,认为其为危险用户,禁止其登录并通知预警管理单元。与此同时,可以在用户指纹匹配成功后,由认证服务器对用户输入的PIN码进一步验证,若验证正确再向用户端反馈认证成功的信息。

4.3 方案验证

与传统认证技术相比,指纹识别的优势在于能够更为可靠地确认用户身份,从而保证用户更为安全地登录云服务系统。基于此,对本文提出的基于指纹识别的云安全认证系统进行了以下安全性验证。

(1) 可识别性

作为当前最为热门的一类模式识别技术,指纹识别正处于快速发展期。随着电子工艺技术以及智能匹配算法的发展,指纹识别越来越多应用于生产生活各个领域。对政府而言,目前指纹鉴定已经被官方司法机构所接受,建立了全球范围的指纹鉴定机构以及罪犯指纹数据库。对民众而言,各类手机终端,如苹果、三星手机以及银行、金融等高密级系统也开始采用指纹识别功能。在市面上现有的指纹仪中,已达到认假率 $FAR < 0.001\%$ 、拒真率 $FRR < 1\%$ 的处理精度。

(2) 可认证性

本文设计的云安全认证系统采用了双向认证机制,参与认证的用户端与云端认证服务器都需要验证对方的身份。用户端和云端在认证过程中处于平等地位,不仅需要用户向云端证明其合法身份后才能访问云端,用户也必须确认云端的合法性才能将关键数据存入其中,从而避免了中间人的恶意攻击,并能够有效防范用户端和云端任何一方的事后抵赖行为。

(3) 机密性

本文设计的基于指纹识别的云安全认证系统通过对称加密算法对会话密钥进行加密,加强用户端与云端之间数据传输的机密性。每次认证过程中用于加密指纹信息的会话密钥均是动态随机生成的,从而保证传输的指纹信息不会泄露。在用户端与云端的通信中,本设计采用了SSL

协议,进一步保证了整个传输过程中数据的安全性。此外,利用云端分布式存储及加密技术,还可以实现云数据库中用户指纹数据的安全存储。

5 结束语

在云计算模式中,用户的数据和计算都由云端服务器进行存储和运行,数据安全性及隐私问题成为云计算发展的重要障碍。用户身份认证作为云服务的第一道安全防线,是云计算应首要解决的安全性问题,否则云端的一切服务都将变得不可信。本文采用指纹识别技术进行身份认证,利用指纹特征唯一性、不变性、不易丢失、遗忘或被伪造等优点,保证用户访问云端的安全性。为了进一步提高系统认证效率,采用了三层B/S架构设计及分布式存储技术。首先由顶层客户服务端进行用户指纹采集、特征值提取及加密,生成认证数据;然后由中间层应用服务层还原认证数据并与指纹模板进行匹配从而确认用户身份;最后底层数据库服务层负责将海量指纹信息根据地域和用户级别进行分布式分类存储。随着指纹识别技术的不断发展以及硬件成本的不断下降,基于指纹识别的云安全认证技术必将获得更为广泛的应用,从而进一步推进云计算行业的发展。

参考文献

- 1 张祥丽. 一种基于指纹识别的云安全登录系统设计. 电视技术, 2013(13):166~171
Zhang X L. Design of cloud security login system based on fingerprint recognition. Video Engineering, 2013(13):166~171
- 2 余彬彬. 动态身份认证系统的研究与实现(硕士学位论文). 上海交通大学, 2008
Yu B B. The research and implementation of the dynamic identity authentication(master dissertation). Shanghai Jiaotong University, 2008
- 3 宁璇. 基于指纹识别与智能卡的身份认证系统设计(硕士学位论文). 北京邮电大学, 2009
Ning X. Design of the identity authentication system based on fingerprint identification and smartcard(master dissertation). Beijing University of Posts and Telecommunications, 2009
- 4 康利山. 云安全中基于身份的认证机制研究(硕士学位论文). 云南大学, 2011
Kang L S. Research on identity-based authentication mechanism in cloud security(master dissertation). Yunnan University, 2011
- 5 罗耀坤. 指纹识别在网络身份认证中的应用研究(硕士学位论文). 东北大学, 2005



Luo Y K. Applied research for fingerprint identification in the field of network status authentication(master dissertation). Northeastern University, 2005.

- 6 程元栋. 指纹识别技术在电子商务安全认证中的应用与研究(硕士学位论文).安徽理工大学, 2009

Chen Y D. Fingerprint recognition technology in E-commerce applications in the security certification and research(master dissertation). Anhui University of Science and Technology, 2009

- 7 何军. 指纹识别技术的研究与应用(硕士学位论文).首都经济贸易大学,2004

He J. The research and application of fingerprint identification technology(master dissertation). Capital University of Economics and Business, 2004

- 8 赵艳超. 指纹识别技术在银行业务系统中的应用(硕士学位论文).浙江大学, 2006

Zhao Y C. The application of fingerprint identification technique in banking system(master dissertation). Zhejiang University, 2006

- 9 姚冰莹. 指纹识别技术在 Web 云存储安全认证中的应用研究(硕士学位论文).广东工业大学,2014

Yao B Y. The application of fingerprint identification technique in Web cloud storage security system(master dissertation). Guangdong University of Technology, 2014

[作者简介]



汤雅妃,女,中国联合网络通信有限公司研究院云计算实验室工程师,主要研究方向为云计算、大数据和信息安全。



张云勇,男,博士后,中国联合网络通信有限公司研究院副院长,国务院特殊津贴专家,中国通信学会会士,主要研究方向为下一代开放网络、移动互联网及业务、云计算和智能终端等。



张尼,男,博士后,中国联合网络通信有限公司研究院云计算实验室高级工程师,主要研究方向为移动互联网安全、云计算安全 and 信息安全。