Journal of Wuhan Polytechnic

电子商务网络安全性策略研究与设计

白有林

（武汉铁路职业技术学院，湖北 武汉 430205）

摘 要：分析了电子商务网络安全现状后，提出了电子商务网络的安全需求，充分阐述了当下几种网络安全策略及方法，提出一种线下与线上有机结合的网络认证策略，即结合生物设别和密码加密技术，为电子商务网络安全提供一种全新的安全策略。

关键词：电子商务；指纹识别；密码技术；网络安全

中图分类号：F713.363 文献标识码：A 文章编号：1671-931X（2014）03-0055-05

引言

随着21世纪的到来，网络时代也伴随着进入人们的生活，国家与国家、企业与企业、人与人都与网络关联起来，时代的变革导致企业或个人的商务交互几乎完全依托于网络，网络的经济交易和运营是目前最为火热的渠道，企业通过互联网推广品牌和推销产品，或者通过WEB技术搭建自己的门户网站，以此让更多的企业和个人关注，促进网上交易的发展，而这种通过互联网交易的方式，我们称为电子商务。

信息作为当今每个国家通讯手段的主要内容之一，其多效用性、普遍性、增值性以及共享性对人类具有重要意义。信息的交互就涉及到了其安全性问题，这也是每个国家应足够重视的部分，当今任何一个国家、企业或个人都将各自的真实信息存于网络中，如何使之具有高安全性，保证各种信息资源不受外界的破坏或干扰。电子商务正是基于信息时代出现的，其安全性尤为重要，我国当前采用的主要技术为加密技术、认证技术和部分交互协议，通过这些技术的应用，确保交互信息不被第三方破坏和干扰，并保证其具有保密性。

实现电子商务的关键是要保证商务活动过程中系统的安全性，即应保证其在向基于Internet的电子交易转变的过程中与传统交易的方式一样安全可靠。电子商务的安全主要采用数据加密和身份认证技术（CA认证）。

一、电子商务安全性需求分析

交易安全是电子商务中所要解决的核心问题之一。电子商务交易平台安全性取决于建立科学、合理的安全体系结构和控制机制，满足其交易安全的需求必须做到以下几点：

（一）信息的保密性

在电子商务平台上面，交易中的信息都是具有保密要求，因为这些内容有些可能涉及公司或企业的重要商业信息，保密性极为重要，因此不能随便被他人获取。在现在的电子商务平台中，一些钓鱼网站往往利用用户的无知获取用户的账户和密码，将银行卡中的金额全部盗空，导致个人或企业经济严重受创。由此可见电子商务平台的保密性极为重要。

（二）交易各方身份的认证

信息化时代，网络交易越来越多，如果确定买卖

收稿日期：2014-05-04

作者简介：白有林（1975-），男，湖北随州人，武汉铁路职业技术学院讲师，工程师，研究方向：高职教育管理、校企合作机制。

双方是否为合法用户，前提是电子商务平台提供一个安全认证机构，使在平台交易的单位或个人都需实名制注册。这样在交易过程中可以确定对方身份，有力保障用户交易安全，打造身份注册认证机制是互联网交易的必须前提。

（三）信息的防抵赖性

在现实生活中，往往交易会出现抵赖，这种现象在互联网上更是层出不穷，如何杜绝此种现象，这就需要电子商务交易平台提供强有力的操作记录和凭证，因此在网络上，系统强制的规定了一些操作步骤，使交易双方都必须完成情况的填写。当双方产生交易时，系统会自动记录交易时间，状态等信息，便于后期查阅，这样有效的保证了交易的可追溯性。市场商情变化万千，一旦成交则不容否认，只有双方均同意终止，此次交易关闭才能成立，防止抵赖事件发生。

（四）信息的完整性、防篡改性

不管是何种方式，电子商务平台作为交易平台，其就应该能保证用户信息和交易信息的完整性。因此交易平台应打造一套有效的服务认证机制，服务于客户，用户的资料不能由第三方随意篡改，必须保证用户的所有信息和交易信息完整，第三方无权修改，只有查阅功能。

通过以上安全需求分析可知，电子商务平台是一款完全保证用户信息安全和交易的平台，在满足用户需求的同时，要构造一款具有认证机制的服务体系，可采用基本加密算法、安全认证手段和安全应用协议等实现服务认证体系。

二、电子商务网络安全策略分析

电子商务在发展过程中遇到各种风险问题，因此针对电子商务的安全方面呈现出几种核心的技术，主要包括：防火墙技术、身份认证技术、密码体制以及电子签名等。

（一）电子签名

电子签名顾名思义就是将现实的签名方法转嫁至网络之上，通过电子数据的签名来模拟，用户在日常的网络生活中所产生的报文信息都会绑定数字签名，这些都可以作为查证的依据，这就是电子签名作为安全技术的一大特点。

（二）密码体制

密码技术基本思想是在加密密钥 Ke 的控制下按照加密算法 E 对要保护的数据（即明文 M）加密成密文 C，记为 C=E(M,Ke)。而解密是在解密密钥 Kd 的控制下按照解密算法 D 对密文 C 进行反变换后还原为明文 M，记为 M=D(C,Kd)。加密体制中的加密技术是一种常用的技术，它在网络电子数据中往往用于数据传输加密、数据存储加密和各种文件信息的加密，是电子商务安全技术使用最为常用和广泛一种技术，加密技术主要分为公钥加密和私钥加密。

1.公钥加密

也是一种非对称密钥加密，初始会有一对密钥，在网络数据传输过程中，发方发出的数据会由一对密钥中的公开密钥进行加密，而收方则使用一对密钥中的私钥进行解密，这样就保证了数据的安全，同时验证了密钥的唯一性，目前常用的公钥加密方法有 RSA 和 EIGamal 等。

2.私钥加密

也被称为对称密钥加密，在网络中往往通过同一密钥去加密和解密的过程称为私钥加密，目前常用的私钥加密有 IDEA 和 DES 等。

（三）认证技术

电子商务平台中的安全认证技术是一项基本需求，而目前电子商务认证技术主要体现在 CA 认证、电子认证，也有些信息安全用到了生物认证方法。生物认证方法有很多，应用的场合也不同，认证技术在发展过程中，比较成熟的有指纹身份认证技术和声纹身份认证，他们通过身份生理特征存在唯一性进行定位设别。

（四）防火墙技术

防火墙作为一种网络数据核查软件，很好的杜绝了网络用户通过非法渠道获取其他网络用户信息，它通过分包和 IP 地址并行校验机制，对外来数据进行一一检查，此种技术很好的保障了内部数据的安全性。目前，防火墙技术主要是分组过滤和代理服务两种类型。

从以上四种网络安全技术特点及应用全面性分析，电子商务安全性需要综合多方面问题进行全面设计，本文在已有技术应用基础之上，结合目前生物认证技术和信息加密体制技术，全面有效的提供电子商务安全性，提出综合技术创新，提高了电子商务的安全机制。

三、指纹密码结合技术的研究与设计

（一）技术原理及设计思路

指纹与密码相结合就需要深入了解两种技术实现的原理，为进一步融合做好技术铺垫，首先指纹作为人体生物特征具有唯一性，而且目前在我国很多笔记本终端厂家都植入指纹识别系统，由此可见指纹识别技术已经发展的非常成熟，本文正是基于此种技术应用与电子商务的身份识别上，指纹识别的流程主要包括以几个环节：指纹采集、图像数据传输、数据处理、特征值提取、配对、保存数据。其中指纹采集主要依托于每个客户终端放置一个指纹录入仪，通过指纹扫描录入图像，再由认证系统对图像进

行分析再处理,获取图像中的关键特征点,以此与已有的指纹数据库进行特征数据比对,确定身份。

密码技术的实现主要针对两部分进行加工,其主要特点是将明文数据通过特定协议或规则进行加密,借助网络传递与接收端,再通过对应协议和规则进行解密,再以明文呈现,由此可见在加密技术应用过程中,最关键的技术体现在加密和解密两个部分。加密和解密都绑定了一个密钥或对应密钥,而密钥是加密技术中的关键,它本质是非常大的数,密钥尺寸用位(bit)表示,在公开密钥加密方法中,密钥尺寸越大,密文就越安全。

为进一步加强指纹身份验证的安全性,保证数据传输过程中不被盗取或盗取也无法获得明文,本文融入了密码体制技术,指纹采集后,采用加密技术对图像进行加密,使用户的指纹信息不被恶意修改,充分提高了认证技术的高可靠性和安全性。总体方案设计流程图如图 1 所示。

指纹与密码体制的相结合主要以数据加密为主,每个过程都采用了加密机制的 RSA 加密和解密,进一步加强了指纹数据传输过程中的安全性,也体现了生物认证技术和密码体制的有机结合的可行性。

(二)新方案的安全性设计

电子商务作为本世纪交易最为流行的平台,其安全是第一位的,往往由于其安全漏洞导致个人信息或企业资金损失,本文基于两种相对成熟技术有机结合,进一步加强了电子商务的安全性。本文所设计的具体方案为:通过线下的指纹扫描入网,再通过分析处理获得用户的指纹特征值,结合加密函数的 RSA 算法产生的一对密钥,利用 KDC 公钥 EPK 实施加密,借助网络上传 KDC 加密文件,到认证系统内部后,进行指纹特征值的比对和校验,认证成功则为用户提供解密方式,允许用户登录电子商务交易平台,否则拒绝用户登录电子商务平台。

采用了加密和解密的密码体制来加强信息安全性,在以往的认证系统总往往出现一些信息的泄露或者被修改,导致系统的安全性降低,也给企业或者机构造成了损失,而本文设计的方案从根本上解决了这一问题。通过对指纹特征值进行加密,上传 KDC,最后由 KDC 对信息进行匹配处理再次加密发送给客户,让用户获得私钥进入安全交易网络,这一完整的加密过程,使信息在网络传输过程中绝对的

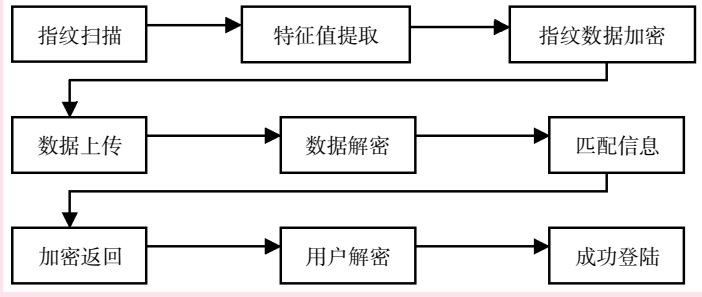

图 1　指纹与加密数据流程图

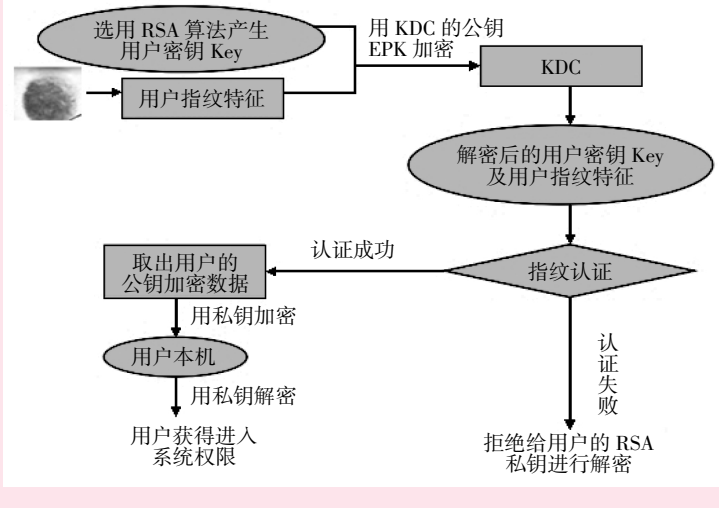

图 2　安全流程图设计

安全，同时采用指纹认证技术可以防止客户抵赖，具有唯一性。具体的安全性设计可以在图 2 中充分地体现出来。

针对新方案的技术的有机结合，主要的安全设计体现在以下几个方面：

1.安全性第一个方面体现在指纹扫描录入后的数据加密，此环节采用了 RSA 算法生成一对密钥，一个公开密钥，一个为私钥。

2. 安全性第二个方面是数据信息上传后再由 KDC 进行二次加密处理，防止过程数据在网络传输中被窃取。

3.安全性第三个方面主要体现在数据加密体制中，实现加密+解密+再加密+再解密的双重加密体制，有效的提高了数据传输的安全性。

指纹加密体制的有机结合体现图如图 3 所示。

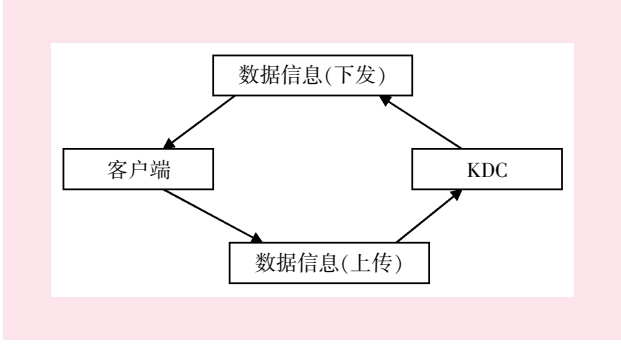

图 3　加密机制体现图

指纹与加密体制的有机结合，采用多层加密的方式，主要是针对黑客会针对 IDEAK 实施枚举法破解，本方案也可以根据用户的实际需求进行的更多层的加密机制调整，进一步提高系统的安全性。

（三）新方案算法设计

指纹与密码技术在电子商务上的应用主要依托其基本的算法实现，而两种技术分别是线下和线上的双重结合，本文通过线下的指纹扫描获取指纹图像信息，由认证系统实施匹配和对比，再由加密技术实施双重加密，实现电子商务的高安全性，下面就新方案的有机结合技术分别介绍其中的算法实现：

1.指纹扫描及图像认证算法的实现

根据目前电子商务业务定制用户特殊交易网络平台，为用户打造特定的指纹输入仪，每个客户端用户提前将自己的指纹扫描入库后，会对应此用户的所有电商平台上的资料。本文的指纹认证算法主要体现在指纹扫描录入后的匹配算法，指纹图像匹配的关键是另个指纹图像的模糊相似细节点的个数统计，进而得到一个衡量相似性的匹配值，认证系统会根据匹配值与设定的阈值进行比较，如果这个匹配值在设定的阈值范围内，证明此两个细节点具有充分的相似程度，可以确定为同一个用户，否则亦然。下面就具体的算法模型进行分析：

首先根据细节点特点建立细节点特征向量，每个细节点建立一个平面坐标，其对应坐标点设为(x^k, y^k)，设细节点末端分叉点为 z^k，每个细节点的阈值为 t，根据匹配算法建立特征向量 $U^k=(x^k,y^k,z^k,t^k)$。其次认证系统对已有的指纹模板建立特征向量和已经扫描过的指纹图像也建立细节点特征向量，其表达式如下：

$$W=\{U_i^P \mid i=1,\cdots,M\} \quad (1)$$

$$C=\{U_j^Q \mid j=1,\cdots,N\} \quad (2)$$

根据两个细节点的特征向量表达式，M/N 是模板指纹和刚输入指纹分别的细节点个数。认证系统通过两个特征向量进行细节点关系匹配，最后统计匹配上的细节点个数，得到一个匹配值 X，将此匹配值与 T（设定的两个指纹细节点相似度最小值），当 X≥T 时，表明两个细节点匹配个数超过预设的值，两个指纹成功匹配。

2.认证系统的第二个认证环节就是对匹配成功的指纹信息的加密和解密，本文的密码体制所采用的加密算法为成熟的 RSA 加密算法

RSA 作为公钥加密技术，它最大的特点就是会产生一个公开密钥和一个私有密钥，它的算法所依据的原理为欧拉定理，在产生密钥的同时分配两大素数，而加密就是将他们相乘作为公钥，再将两大素数进行欧拉定理运算，经过一定的处理得到私有密钥。

$$N=p*q \quad p,q\in(100bit) \quad (3)$$

$\Phi(N)=(p-1)(q-1)$ $\Phi(N)\leqslant N$(N 互为素数的个数)

(4)

$$d=e-1(\mathrm{mod}\Phi(N)) \quad e\in[0,\Phi(N)-] \quad (5)$$

PK=(e,N)，SK=(d,N)(N 的长度大于 512 bit

(6)

其中 p，q 为安全素数，e 与 $\Phi(N)$互为素数，PK 和 SK 分别为一对密钥，加密和解密公式为：

$$Y=Xe(\mathrm{mod}N) \quad X,Y\in M(整数) \quad (7)$$

$$X=Yd(\mathrm{mod}\ N) \quad X,Y\in M(整数) \quad (8)$$

通过上述分析，本论文阐述了在认证系统实现过程中主要采用了指纹细节点匹配算法和 RSA 加密算法，经过双层加密校验机制，有效的提高了系统在网络信息交互过程中的安全性。

四、总结

电子商务模式相对传统商务模式，具有便捷、高效的特点。本文提出了一种基于指纹加密的网络身份认证方案，利用指纹线下扫描方式录入用户生物特征的惟一性和方便性，经过双重认证技术（指纹匹配和加密技术），有效的提高了系统安全性，使此方案具有一定的创新性和实用性。为信息化电子商务

带来了全新的安全保障，通过一系列的操作后，在电子商务中起到了信息安全、双重验证、实时性、机密性以及完整性。根据系统结构图的分析可实现电子商务的正常运行，为电子商务的运营提供了强有力的保障。

参考文献：

[1] 杨千里，王育民，等.电子商务技术与应用[M].北京：电子工业出版社，1999.

[2] 殷国宴.电子商务中的身份认证技术研究[M].西安：西安电子科技大学出版社，2006.

[3] 罗雅丽.一种基于指纹加密的网络身份认证方案[J].现代电子技术，2007，(7).

[4] 张华.电子商务安全认证技术的研究与应用[J].江门职业技术学院学报，2006，(2).

[5] 殷晓虎.电子商务的安全问题及对策研究[M].西安：西安科技大学出版社，2006.

[6] 段正敏.身份认证技术研究与实现[D].重庆：重庆大学软件学院，2004.

[责任编辑：胡大威]

Research and Design of Electronic Commerce Network Security Strategy

BAI You-lin

(Wuhan Railway Vocational College of Technology, Wuhan 430205, China)

Abstract: This paper, a comprehensive analysis of the electronic commerce network security, proposes the requirements for network security of electronic commerce, fully expounds several network security strategies and methods at present, in the face of the electronic commerce network security problem, this paper presents a line network authentication strategy which combines biological equipment and pass word encryption technology and provides a new security strategy for e-commerce network security.

Key words: electronic commerce, fingerprint, password technology, network security

（上接第 50 页）

参考文献：

[1] 中国互联网络信息中心. 第 33 次中国互联网络发展状况统计报告[R/OL].http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/p020140305346585959798.pdf，2014-01-16.

[2] 鲜于建川，隽志才.出行链与出行方式相互影响模式[J].上海交通大学学报，2010，44(6)：792-796.

[3] 谭家美，徐瑞华.影响出行链构成的多因素分析[J].同济医学学报(自然科学版)，2009，37(10)：1340-1344.

[4] Card S, Mackinlay J, Shneiderman B. Readings in Information Visualization: Using Vision to Think [J]. Morgan Kaufmann, 1999.

[5] Spence R.信息可视化：交互设计(原书第 2 版)[M].北京：机械工业出版社，2012：38-39.

[责任编辑：胡大威]

Research on the Visualization of Web life Service Information based on Relative position

HUANG Jing

(Wuhan Polytechnic, Wuhan 430074,China)

Abstract: This paper designs an interactive visualization prototype for web life service information, which utilizes relative position based web life service information organization and combines trip chain theory and Bertin coding principle in information visualization technology. Then the paper conducts an empirical study of this interactive prototype from the perspective of group purchase web life service information in order to test the feasibility and interactivity of this prototype and present its advantages.

Key words: information visualization, Bertin coding principle, web life service information, relative position