Journal of Information Technology Management
ISSN: 2008-5893
EISSN: 2423-5059
Vol. 9, No. 2; PP. 355 - 378
Summer 2017

University of Tehran
Faculty of Management

Fuzzy Group Decision Making Model for Identifying and Ranking of Success Factors in Fraud Prevention in Iranian E-banking

Alireza Alizadeh [1], Mehri Chehrehpak [2]

Abstract: With increasing use of e-banking system in Iranian banking sector, ignoring the issue of fraud in the system will be very costly for banks and e-banking customers. Fraud in e-banking is due to some security problems (such as weakness in access control systems and inadequate internal control). So, identifying success factor in fraud prevention in e-banking can be useful for e-banking system developers to improve these systems security. In this paper we have tried to identify and rank these success factors for fraud prevention in e-banking systems. For this purpose, we first review the literature to find potential factors, then identified factors were weighted by using fuzzy group multi criteria decision-making model and experts' judgment. The results show that for elimination fraud in e-banking systems it is necessary to pay attention to technical, operational, strategic and financial factors respectively.

Key words: ***Analytical hierarchy process (AHP), Electronic banking, Fraud, Fuzzy group decision making, Security.***

1. PhD. of Industrial Engineering, Sharif University of Technology, Tehran, Iran
2. MSc, in Industrial Management, South Tehran Branch, Islamic Azad University, Tehran, Iran

Submitted: 04 / October / 2016
Accepted: 10 / April / 2017
Corresponding Author: Alireza Alizadeh
Email: aralizadeh@gmail.com

مدیریت فناوری اطلاعات
Journal of Information Technology Management
دانشکدهٔ مدیریت دانشگاه تهران
دورهٔ ۹، شمارهٔ ۲
تابستان ۱۳۹۶
صص. ۳۷۸- ۳۵۵

تصمیم‌گیری گروهی فازی برای شناسایی و اولویت‌بندی عوامل موفقیت مقابله با تقلب‌های بانکداری الکترونیک در ایران

علیرضا علیزاده[۱]، مهری چهره پاک[۲]

چکیده: با افزایش بهره‌مندی از نظام‌های نوین بانکی و بانکداری الکترونیک در کشور، تقلب در این سیستم‌ها موضوعی است که مقابله‌نکردن با آن می‌تواند هزینه‌های بسیاری برای نظام بانکی و مشتریان بانکداری الکترونیک در پی داشته باشد. تقلب در سیستم بانکداری الکترونیکی نتیجهٔ بی‌توجهی به برخی مشکلات امنیتی (از ضعف در سیستم‌های دسترسی تا کنترل‌های داخلی نامناسب) است. به‌طبع، شناسایی عوامل موفقیت مقابله با تقلب، می‌تواند برای توسعه‌دهندگان سیستم‌های بانکی در افزایش ضریب امنیتی این سیستم‌ها بسیار مفید باشد. در این مقاله تلاش شده است عوامل موفقیت مقابله با تقلب‌های بانکداری الکترونیک، شناسایی و وزن‌دهی شوند. به این منظور ابتدا با مرور ادبیات، عوامل بالقوهٔ موفقیت در مقابله با تقلب در بانکداری الکترونیک شناسایی شدند، سپس با استفاده از تصمیم‌گیری چند معیارهٔ گروهی فازی و بهره‌مندی از نظر خبرگان حوزهٔ بانکی، عوامل یاد شده مقایسهٔ زوجی شده و وزن آنها به‌دست آمد. نتایج تحقیق نشان می‌دهد برای مقابله با تقلب در بانکداری الکترونیک، به‌ترتیب باید به عوامل فنی، عملیاتی، استراتژیک و مالی توجه کرد.

واژه‌های کلیدی: امنیت، بانکداری الکترونیک، تصمیم‌گیری گروهی فازی، تقلب، فرایند تحلیل سلسله‌مراتبی (AHP).

۱. دکتری مهندسی صنایع، دانشکدهٔ مهندسی صنایع، دانشگاه صنعتی شریف، تهران، ایران
۲. کارشناسی ارشد مدیریت صنعتی، دانشگاه آزاد، واحد تهران جنوب، تهران، ایران

تاریخ دریافت مقاله: ۱۳۹۵/۰۷/۱۳
تاریخ پذیرش نهایی مقاله: ۱۳۹۶/۰۱/۲۱
نویسندهٔ مسئول مقاله: علیرضا علیزاده
E-mail: aralizadeh@gmail.com

مقدمه

خدمات بانکداری الکترونیک، دسته‌ای از خدمات بانکی است که بانک‌ها به مشتریان حقیقی یا حقوقی در بستر تلفن ثابت یا همراه و اینترنت ارائه می‌دهند (ریبانا کابالیناس، مونوس لیوا، سانچز فرناندز و ویدما دل‌یزوز، ۲۰۱۶). با توجه به توسعهٔ اینترنت و ابزارهای بانکداری الکترونیک در سال‌های اخیر، به‌طبع خدمات ارائه‌شده در این بسترها نیز نسبت به سال‌های گذشته تغییرات شایان توجهی داشته است (پارامسوار، دیر و دیر، ۲۰۱۷). ارائهٔ خدمات بانکی به‌صورت الکترونیکی بسیار ارزان‌تر از روش‌های سنتی است (پیکارینن، پیکارینن، کارجالوتو، پاهنیلا، ۲۰۰۴؛ ساتیه، ۱۹۹۹). از این رو عجیب نیست که امروزه بسیاری از بانک‌ها به‌دنبال توسعهٔ خدمات بانکداری الکترونیک هستند. با توجه به این مسئله و اینکه به نظر می‌رسد خدمات بانکداری الکترونیکی در آینده توسعهٔ بیشتری نیز داشته باشد، لازم است به مسائل امنیتی این حوزه توجه ویژه‌ای شود (شاه، ۲۰۱۶).

تقلب در بانکداری الکترونیک در بستر خدمات الکترونیک و به‌صورت برخط[1] اتفاق می‌افتد و حاصل آن، انتقال پول الکترونیکی از یک حساب به حساب دیگر، به‌صورت نامشروع و غیرقانونی است. امروزه حجم زیادی از معاملات و نقل و انتقالات پولی و مالی در سطح اینترنت و در بستر الکترونیکی انجام می‌شود و رشد روزافزون این خدمات و تراکنش‌ها از یک طرف و ناشناس ماندن مجرمان در بستر اینترنت از طرف دیگر، موجب تشویق و تحریک متقلبان و شیادان برای ورود به این حوزه می‌شود (لکفلد، کلیمانس و استول، ۲۰۱۶).

خسارت‌های غیرمستقیمی که متقلبان به صنعت بانکداری و سازمان‌های مالی وارد می‌کنند، بسیار بیشتر از رقمی است که این سازمان‌ها به‌طور مستقیم متضرر می‌شوند (سکسانا و آگاروال، ۲۰۱۶). برای نمونه در سال‌های گذشته، بازارهای مالی ایالت متحده با افشای متعدد اعمال متقلبانهٔ برخی شرکت‌ها، به‌طور جدی متضرر شده‌اند. ورلدکام[2]، انرون[3]، آدلفیا[4]، گلوبال کروسینگ[5] و تیکو[6]، فقط تعداد اندکی از رسوایی صورت‌های مالی هستند که بازار سهام ایالات متحده را دچار نوسان کردند و باعث سلب اعتماد عمومی در این حوزه شدند. از سوی دیگر، این رسوایی‌ها، زیان‌های جبران‌ناپذیری نیز به سرمایه‌گذاران وارد کرده و باعث از بین رفتن پس‌انداز

---

1. Online
2. WorldCom
3. Enron
4. Adelphia
5. Global Crossing
6. Tyco

افراد، مزایای بازنشستگی، آموزش دانشگاهی و امنیت آیندهٔ آنها شده است (البرچت، البرچت و البرچت، ۲۰۰۸).

این مسائل باعث شده که در سال‌های اخیر، توسعه‌دهندگان سیستم‌های بانکداری الکترونیکی توجه ویژه‌ای به مسائل امنیتی و روش‌های مقابله با تقلب داشته باشند (سان و داویدسون، ۲۰۱۵). در این مسیر شناسایی عوامل موفقیت مقابله با تقلب یکی از مسائلی است که می‌تواند توسعه‌دهندگان این سیستم‌ها و مدیران بانکداری الکترونیک را نسبت به رفع این مشکلات یاری کند (عثمان و شاه، ۲۰۱۳). از این رو طی سال‌های گذشته تحقیقات بسیاری در حوزهٔ شناسایی عوامل موفقیت مقابله با تقلب در بانکداری الکترونیکی صورت گرفته است که از آن جمله می‌توان به مراجع عثمان و شاه (۲۰۱۳) و سکسانا و آگاروال (۲۰۱۶) اشاره کرد.

یکی از مسائلی که در تعیین و اولویت‌بندی عوامل موفقیت مقابله با تقلب در بانکداری الکترونیکی باید در کانون توجه قرار گیرد، این است که اغلب این عوامل، به‌دلیل تفاوت‌های موجود بین زیرساخت‌های فرهنگی، قانونی، مالی و تکنولوژی، در کشورهای مختلف و شرایط گوناگون متفاوت از هم است (اوکپارا، ۲۰۰۹) و ممکن است عاملی که در یک کشور به‌عنوان عاملی کلیدی مقابله با تقلب شناخته می‌شود، در کشوری دیگر اهمیت کمتری داشته باشد. برای نمونه در تحقیق زومیرا (۲۰۱۴) عاملی مثل تخصیص منابع مالی لازم برای مقابله با تقلب در کشوری نظیر زیمبابوه، مهم‌ترین عامل برای مقابله با تقلب شناخته شده است، حال آن که به گفتهٔ محقق، این موضوع در کشورهای پیشرفته، در این حد مهم نیست. در خصوص زیرساخت‌های تکنولوژیک نیز سایمون (۲۰۰۴) به زیرساخت‌های فیزیکی و ارتباطی اشاره کرده و می‌گوید که این زیرساخت‌ها در کشورهای در حال توسعه نسبت به کشورهای پیشرفته ضعیف‌ترند و کل مسائل مربوط به بانکداری الکترونیک و از جمله امنیت را تحت تأثیر قرار می‌دهند.

در ایران نیز در سال‌های گذشته بانک‌ها از بانکداری الکترونیک استقبال کرده‌اند و خدمات مختلف بانکداری الکترونیکی نظیر دستگاه‌های خودپرداز (ATM)، بانکداری اینترنتی، بانکداری همراه و... را برای مشتریان فراهم آورده‌اند. در این گذرگاه، علی‌رغم سیاست‌های امنیتی بانک‌ها که روزبه‌روز در حال افزایش هستند، متأسفانه مقولهٔ تقلب در فضای بانکداری کشور روزانه بسیاری از مشتریان نظام بانکی را قربانی خود می‌کند (راسخی، ۱۳۹۳). بر اساس گزارش‌های پلیس فضای تولید و تبادل اطلاعات ناجا (فتا)، رتبهٔ نخست جرایم فضای سایبری کشور، مربوط به برداشت از حساب بانکی است که نتیجهٔ بی‌مبالاتی مالکان این حساب‌ها در نگهداری رمزها، سوء استفادهٔ اینترنتی از حساب‌ها یا نفوذ هکرها به شبکهٔ بانکی و برداشت پول است. بر اساس

گزارش‌ها، هتک حیثیت و فیشینگ، در رتبه‌های بعدی جرایم سایبری کشور قرار دارند (پوررضا، ۱۳۹۴).

از این رو به نظر می‌رسد، مقولهٔ تقلب و شناسایی عوامل موفقیت تقلب در حوزهٔ بانکداری الکترونیک یکی از مسائل بسیار مهم است که باید در کانون توجه قرار گیرد. متأسفانه پس از مرور پیشینهٔ تحقیقات انجام‌شده در کشور مشخص شد با اینکه در مراجعی به مقولهٔ تقلب در بانکداری الکترونیک پرداخته شده است (برای مثال: محقر، لوکس، حسینی و منشی، ۱۳۸۷؛ دامغانیان و کجوری، ۱۳۹۱؛ وثوق، تقوی‌فرد و البرزی، ۱۳۹۳؛ موسوی، زنوز و حسن‌پور، ۱۳۹۴؛ تقوا، منصوری، فیضی و اخگر، ۱۳۹۵؛ صالحی و علیپور، ۲۰۱۰)، تحقیقی که به موضوع عوامل موفقیت در مقابله با تقلب و وزن‌دهی و اولویت‌بندی این عوامل پرداخته باشد، وجود ندارد. به‌طبع، اجرای این گونه تحقیقات، می‌تواند بانک‌ها و توسعه‌دهندگان سامانه‌های بانکداری الکترونیک را در توسعهٔ سامانه‌های امن یاری کند.

تحقیق حاضر به‌منظور رفع این شکاف پژوهشی و شناسایی و وزن‌دهی به عوامل موفقیت برای مقابله با تقلب در بانکداری الکترونیک در ایران انجام گرفته است. به این منظور در ادامهٔ این مقاله با مروری بر ادبیات تحقیق، مطالعات پیشین در این عرصه بررسی می‌شود؛ سپس روش تحقیق ارائه خواهد شد. بخش بعد به معرفی روش تصمیم‌گیری گروهی به‌کار رفته در تحقیق اختصاص یافته است. در بخش یافته‌ها نیز نتایج تحقیق و وزن‌دهی مربوط به عوامل بیان می‌شود. بخش آخر نیز به نتیجه‌گیری تحقیق اختصاص دارد.

پیشینهٔ پژوهش

از زمان مطرح شدن مفاهیم بانکداری الکترونیک، یکی از موضوعاتی که همواره توجه محققان را به خود جلب کرده، چالش‌های پیش روی این سبک از بانکداری بوده است. این چالش‌ها اغلب فناوری، محدودیت‌های مالی و پذیرش تکنولوژی استفاده از سیستم جدید تهدیدهای امنیتی، موانع فرهنگی، دسترسی محدود به اینترنت و قوانین و مقررات مربوطه را شامل می‌شوند (فالزون و گاردنر، ۲۰۱۶). بر اساس تحقیق انجام‌شدهٔ آوتا (۲۰۱۰) امنیت، کاربرپسندبودن، مدیریت صف[1]، در دسترس‌بودن، عوامل زمانی و انتقال مالی، عوامل مهم در استقرار بانکداری الکترونیکی هستند که در این بین، امنیت مهم‌ترین عامل شناخته شده است. مراجع دیگری نیز مانند اونگ و لین (۲۰۱۵)، منتظمی و صارمی (۲۰۱۵) این مسئله را تأیید کرده‌اند.

1. Queue management

ضعف امنیتی در سیستم‌های بانکداری الکترونیک، زیان‌های مالی، جرایم سنگین توسط قانون‌گذاران و دستگاه‌های حاکمیتی و تبلیغات منفی را در پی خواهد داشت (عثمان و شاه، ۲۰۱۳)، بنابر این اهمیت، توجه به مسائل امنیتی بیش از پیش خودنمایی می‌کند. در این مسیر تقلب‌های بانکی و جلوگیری از وقوع آنها یکی از موضوعاتی است که ارتباط تنگاتنگی با مفهوم امنیت دارد (عثمان و شاه، ۲۰۱۳). از سوی دیگر، به‌طور کلی تمایل به تقلب در سیستم‌های با تراکنش زیاد و بدون قواعد مناسب شناسایی و ردیابی کاربران، افزایش می‌یابد (روبردز، ۱۹۹۸). از این رو، مؤسسه‌های مالی باید نسبت به بهبود مستمر امنیت سیستم‌های بانکداری الکترونیک و مقابله با تقلب اقدام کنند و خطر از دست دادن مشتریان خدمات بانکداری الکترونیک خود را کاهش دهند (گیلز، ۲۰۱۰).

در ادبیات تحقیق تعریف جامع و کاملی در خصوص تقلب که تمام محققان آن را پذیرفته باشند، وجود ندارد؛ اما از نظر بسیاری از محققان، تقلب فریب غیرقانونی است که به سود مالی یا شخصی منجر می‌شود (عثمان و شاه، ۲۰۱۳). بر این اساس، می‌توان تقلب بانکی را استفادهٔ عمدی از اطلاعات نادرست برای دسترسی به دارایی بانک‌ها تعریف کرد (عثمان و شاه، ۲۰۱۳). بر اساس یافته‌های بنجامین و سامسون (۲۰۱۱)، انواع تقلب‌هایی که اغلب مؤسسه‌های مالی آنها را تجربه می‌کنند، عبارت‌اند از: تقلب فروش، تقلب خرید، تقلب پرداخت و تقلب ATM.

در خصوص عوامل موفقیت مقابله با تقلب، تحقیقاتی توسط پژوهشگران پیشین صورت گرفته است که شاید یکی از مهم‌ترین آنها تحقیق عثمان و شاه (۲۰۱۳) باشد. در این مقاله محققان عوامل موفقیت مقابله با تقلب را در چهار دستهٔ عوامل استراتژیک، عوامل مدیریتی، عوامل عملیاتی و عوامل فنی طبقه‌بندی کردند، ولی به اولویت‌بندی این عوامل نپرداختند. این دسته‌بندی در پژوهش حاضر نیز استفاده می‌شود و تلاش خواهد شد، عوامل موفقیت شناسایی‌شده در قالب این چهار دسته ارائه شود.

نخستین دسته از عوامل موفقیت در مقابله با تقلب‌های بانکی، عوامل فنی است (عثمان و شاه، ۲۰۱۳). بانک‌ها و مؤسسه‌های مالی به‌طور دائم در حال ارائهٔ خدمات نوین امنیتی برای از بین بردن تقلب در بانکداری الکترونیک هستند، اما به نظر می‌رسد اقدامات صورت‌گرفته هنوز نتوانسته است تقلب‌های این حوزه را به‌طور کامل از بین ببرد (رانا و باریا، ۲۰۱۵)، در نتیجه به‌منظور بهبود امنیت سیستم‌های بانکداری الکترونیکی، نیاز به تحقیقات جدید در این حوزه احساس می‌شود.

در حوزهٔ عوامل فنی، بهبود سیستم‌های احراز هویت و استفاده از بیومتریک‌ها[1]، یکی از عوامل موفقیت ارائه‌شده در تحقیقات پیشین برای مقابله با تقلب است (آکینیمی، اوموگبادگون و اویلامی، ۲۰۱۱). در توجیه این مسئله می‌توان به این نکته اشاره کرد که فیشینگ[2] یکی از سازوکارهایی است که متقلبان از آن برای به‌دست آوردن اطلاعات کاربری مشتریان برای اهداف خود استفاده می‌کنند. فاطیما (۲۰۱۱) بیان می‌کند که بیش از ۳۵ درصد مؤسسه‌های مالی هدف اقدامات فیشینگ قرار می‌گیرند و این چالش موجب از دست رفتن هزاران دلار در سال می‌شود. او پیشنهاد می‌کند که از بیومتریک‌ها برای از بین بردن این مشکل استفاده شود. در این مسیر استفاده از کلمه و رمز عبور برای شناسایی مشتریان بانکداری الکترونیک، احتمال سرقت اطلاعات را افزایش می‌دهد و باید روش‌های دیگری نیز برای احراز هویت به‌کار برد (موسکویچ و همکاران، ۲۰۰۹). فناوری بیومتریک (نظیر اثر انگشت و روش تایپ‌کردن با کیبورد[3]) با توجه به ویژگی‌های منحصر به فرد هر مشتری می‌تواند برای شناسایی استفاده شود و استفادهٔ آن در عمل، احراز هویت و انکارناپذیری اطلاعات را در فضای بانکداری الکترونیک با دقت بسیار زیادی تضمین می‌کند (باتاچارایا، رانجان، الیشروف و چوی، ۲۰۰۹). بنابراین استفاده از این تکنولوژی در کاهش تقلب‌های بانکی، نقش اساسی دارد.

نکتهٔ دیگری که در خصوص روش‌های احراز هویت باید به آن توجه شود، این است که این روش‌ها باید برای بانک‌ها و مؤسسه‌های مالی از نظر فنی و اقتصادی توجیه‌پذیر باشند (موردوچ و اندرسون، ۲۰۱۰). هرچند روش‌های بیومتریک، امتحان خود را در شناسایی مشتری از نظر فنی برای پیشگیری از تقلب به خوبی پس داده‌اند، از نظر اقتصادی در خصوص توجیه‌پذیر بودن آنها بین محققان بحث جدی وجود دارد (عثمان و شاه، ۲۰۱۳).

در میان مسائل فنی، موضوعاتی مانند رمزنگاری داده‌های بانکداری الکترونیک (گانسان، ۲۰۰۹؛ روبردز، ۱۹۹۸)، مقیاس‌پذیربودن سیستم‌های امنیتی (موسکویچ و همکاران، ۲۰۰۹)، کاهش امکانات و اختیارات مدیریت سیستم (واندوملە، ۲۰۱۰)، کاربر دوست‌بودن[4] سیستم‌ها (واندوملە، ۲۰۱۰) و تجمیع و یکپارچگی راه حل‌ها (عثمان و شاه، ۲۰۱۳) نیز، در تحقیقات پیشین به‌عنوان راهکارهایی برای مقابله با تقلب پیشنهاد شده‌اند.

با گذر از عوامل فنی، عثمان و شاه (۲۰۱۳) دستهٔ عوامل دیگری موسوم به عوامل مدیریتی را مورد توجه قرار دادند و «حمایت مدیریت ارشد» را یکی از این عوامل معرفی کردند. این عامل

---

1. Biometrics
2. Phishing
3. Keystroke dynamics
4. User friendliness

که به‌عنوان یکی از عوامل موفقیت بانکداری الکترونیک مطرح است، در این حوزه نیز نقش کلیدی دارد (عثمان و شاه، ۲۰۱۳). در توجیه اهمیت این عامل باید اشاره کرد که در بانکداری الکترونیک به‌منظور پیشگیری از تقلب، روش‌های مختلفی همچون رمزنگاری (گانسان، ۲۰۰۹)، کلمهٔ عبور (جانسون و مور، ۲۰۰۷) و کلمات عبور یک بار مصرف (ماتیوانان و کاویتا، ۲۰۱۵) استفاده می‌شود. بنابراین تغییر از یک سیاست به سیاست دیگر، اجتناب‌ناپذیر است و بدون حمایت مدیر ارشد سازمان با دشواری‌های بسیاری مواجه می‌شود (عثمان و شاه، ۲۰۱۳). عثمان و شاه (۲۰۱۳) همچنین بر این نکته تأکید دارند که مدیران ارشد باید در راستای این تغییرات سیاستی، زمینهٔ لازم را میان کارکنان نظام بانکی فراهم آورند و نظام‌های مدیریت تغییرات را در راستای مقابله با تقلبات در سازمان ایجاد کنند. در دستهٔ عوامل مدیریتی، عامل دیگری که توسط ابوعلی و ابوعدوس (۲۰۱۰) شناسایی شده است، تخصیص منابع کافی برای مقابله با تقلب در نظام‌های بانکداری است.

عوامل عملیاتی، عوامل دیگری است که برای مقابله با تقلب باید در نظر گرفته شود (عثمان و شاه، ۲۰۱۳). استفاده از نظام‌های حسابرسی داخلی در بانک‌ها، از مهم‌ترین این عوامل است. بر اساس گزارش کرام، فرگوسن و مورونی (۲۰۰۸)، سازمان‌هایی که نظام‌های حسابرسی داخلی مناسبی دارند، در مقایسه با سایر سازمان‌ها، به احتمال بیشتری نسبت به شناسایی و گزارش تقلب‌های بانکی اقدام می‌کنند. محققان همچنین اشاره کرده‌اند سازمان‌هایی که بخشی از فعالیت‌های حسابرسی را به‌صورت داخلی انجام می‌دهند، نسبت به سازمان‌هایی که فرایند حسابرسی را به‌طور کلی برون‌سپاری می‌کنند، در شناسایی تقلب‌ها کاراترند. البته باید توجه داشت که انجام کلیهٔ فرایندهای حسابرسی به‌صورت داخلی بسیار پرهزینه‌تر از برون‌سپاری است و مواردی به چشم‌پوشی حسابرسان از برخی تقلب‌های مدیران منتج می‌شود (سلامه، الوشاه، النسور و الهیاری، ۲۰۱۱). بنابراین شاید بهتر است که سازمان‌ها نسبت به این امر دقت بیشتری داشته باشند و از تلفیق برون‌سپاری و انجام امور حسابرسی داخلی استفاده کنند.

نتایج بررسی‌ها گویای آن است که در بسیاری از موارد، کارکنان بانکی با متقلبان در تعامل هستند. این مسئله از آن جهت حائز اهمیت است که این افراد به‌صورت مستقیم به سیستم‌های بانکی و اطلاعات فردی مشتریان دسترسی دارند. بر اساس گزارش رسمی FBI، عمدهٔ تقلب‌های بانکی در بانک‌های آمریکا، توسط کارکنان بانکی صورت می‌گیرد (باتن و گی، ۲۰۱۳). محققان بسیاری به بررسی این موضوع پرداخته‌اند که چرا کارکنان بانک‌ها در چنین اقداماتی شرکت می‌کنند. نتایج این تحقیقات نشان می‌دهد نابرابری‌های پرداختی به کارکنان و نداشتن امنیت شغلی، اثر شایان توجهی بر این اقدامات متقلبانه دارد (بنجامین و سامسون، ۲۰۱۱). برای مقابله

با این امر، ریزاردی (۲۰۰۸) بر حفاظت کامل داده‌های مشتریان به‌عنوان عاملی برای مقابله با تقلب تأکید دارد. همچنین محققانی مانند کرام، فرگوسن و مورونی (۲۰۰۸) نیز به وجود نظام‌های ممیزی داخلی منظم کارکنان به‌عنوان عاملی دیگر برای مقابله با تقلب اشاره کرده‌اند. عثمان و شاه (۲۰۱۳) نیز نظام‌های کنترل داخلی شدید بانکی را عامل دیگری در مقابله با این دسته از تقلب‌ها می‌دانند.

عثمان و شاه (۲۰۱۳) در دستهٔ عوامل عملیاتی، به ایجاد تیم‌های امنیتی متخصص در بانک‌ها برای شناسایی و مقابله با تقلب تأکید دارند. این تیم‌ها باید نسبت به شناسایی تقلب‌ها و مقابله با آنها واکنش سریعی داشته باشند. آنان ارائهٔ خدمات به مشتری به‌صورت واکنشی[1] را عامل موفقیت دیگری برای مقابله با تقلب برشمردند؛ به این معنا که بانک‌ها باید ضمن شناسایی دائم نیازهای مشتریان، نسبت به ارائهٔ خدمات مربوطه اقدام کنند و زمینهٔ سوء استفادهٔ متقلبان از شکاف‌های موجود را به حداقل برسانند.

دستهٔ عوامل استراتژیک، آخرین دسته از عواملی است که عثمان و شاه (۲۰۱۳) به آن اشاره کرده‌اند. برخی از تحقیقات، آسیب‌پذیری مشتریان بانکی از تقلب را نشئت گرفته از مسائلی نظیر آموزش و ویژگی‌های جغرافیایی می‌دانند (مانند چوپلین، استارک و احمد، ۲۰۱۱). نتایج تحقیقات ریزاردی (۲۰۰۸) گویای این است که آموزش‌های ارائه‌شده به مشتریان برای محافظت اطلاعات شخصی، در مقابله با تقلب‌های انجام‌شده در حوزهٔ کارت‌های بانکی نقش اساسی دارد.

ایگوه (۲۰۱۱) بر عوامل اقتصادی ـ اجتماعی مانند بیکاری و فقر به‌عنوان عوامل ایجادکنندهٔ تقلب تأکید دارد و در نظر گرفتن اهمیت عوامل اقتصادی ـ اجتماعی در مقابله با تقلب را ضروری می‌داند. اقدام امنیتی دیگر نیز در مقابله با تقلب، استفاده از سازمان‌های واسطه بین مشتری و بانک‌هاست. در این حالت، محرمانگی، یکپارچگی و احراز هویت توسط عوامل سوم صورت می‌گیرد و مشتریان به سیستم‌های بانکی دسترسی مستقیم ندارند (تان و همکاران ، ۲۰۰۲).

همچنین ایجاد روش‌هایی برای ارتباطات و دسترسی به‌موقع مدیران ارشد بانک به اطلاعات، به‌منظور اتخاذ تصمیمات مدیریتی در مقابله با تقلب‌های بانکی، به‌عنوان یکی از عوامل مقابله با تقلب (کوسکوساس، ۲۰۱۱)، استفاده از مشاوران و متخصصان حوزهٔ بانکداری الکترونیک در طراحی خدمات و شناسایی روش‌های مقابله با تقلب (ابوبکر، کومبس، جایاواردنا و هانت، ۲۰۱۰)، ایجاد نظام‌های مناسب برای یادگیری سازمانی در خصوص مقابله با تقلب (روبردز، ۱۹۹۸)، استفاده از سیاست‌ها، روش‌ها و کنترل‌های تطبیقی (عثمان و شاه، ۲۰۱۳) و بهره‌مندی از داده‌های تاریخی و ابزارهای هوش تجاری برای تعیین احتمال تقلب در معاملات (فدریزی،

1. Responsive

مولیناری و ونتره، ۲۰۰۴) نیز می‌تواند در زمرهٔ عوامل موفقیت مقابله با تقلب در بانکداری الکترونیک قرار گیرد.

با توجه به آنچه اشاره شد، جدول ۱ نتایج مرور ادبیات و عوامل موفقیت شناسایی‌شده از مرور ادبیات را در چهار دسته عوامل استراتژیک، مدیریتی، عملیاتی و فنی ارائه می‌کند.

جدول ۱. عوامل شناسایی‌شده از مرور ادبیات

دسته‌بندی	عامل موفقیت	مرجع
عوامل استراتژیک	ایجاد روش‌هایی برای ارتباطات و دسترسی به‌موقع مدیران به اطلاعات برای اتخاذ تصمیمات مدیریتی در مقابله با تقلب‌های بانکی	عثمان و شاه، ۲۰۱۳؛ کوسکوساس، ۲۰۱۱
	ارائهٔ آموزش‌های کافی به کاربران خدمات بانکداری الکترونیک در خصوص تقلب‌های ممکن، به‌منظور کاهش آسیب‌پذیری	چوپلین، استارک و احمد، ۲۰۱۱؛ ابرو و همکاران، ۲۰۱۵
	انجام مطالعات اجتماعی و اقتصادی مناسب قبل از راه‌اندازی خدمات بانکداری جدید	ایگوه، ۲۰۱۱
	استفاده از مشاوران و متخصصان حوزهٔ بانکداری الکترونیک در طراحی خدمات و شناسایی روش‌های مقابله با تقلب	آدامز، ۲۰۱۰؛ ابوبکر، کومبس، جایاواردنا و هانت، ۲۰۱۰
	ایجاد نظام‌های مناسب برای یادگیری سازمانی در خصوص مقابله با تقلب	روبردز، ۱۹۹۸
	استفاده از سیاست‌ها، روش‌ها و کنترل‌های تطبیقی	عثمان و شاه، ۲۰۱۳
	استفاده از اشخاص ثالث متخصص برای انجام معاملات آنلاین به‌منظور افزایش محرمانگی	تان، تیتکوف و پوسلاند، ۲۰۰۲
	استفاده از داده‌های تاریخی و ابزارهای هوش تجاری برای تعیین احتمال تقلب در معاملات	فدریزی، مولیناری و ونتره، ۲۰۰۴
عوامل مدیریتی	اختصاص منابع مالی برای مقابله با تقلب	ابوعلی و ابوعدوس، ۲۰۱۰
	ایجاد آمادگی میان مدیران و کارکنان بانکی برای مقابله با تغییرات در راستای خدمات جدید بانکداری الکترونیک	عثمان و شاه، ۲۰۱۳
	حمایت مدیران ارشد سازمان از سیاست‌های مقابله با تقلب	عثمان و شاه، ۲۰۱۳
	ایجاد نظام‌های مدیریت تغییرات و تغییرات سازمانی کافی در راستای مقابله با تقلب‌ها	عثمان و شاه، ۲۰۱۳
عوامل عملیاتی	حسابرسی داخلی دقیق بانک‌ها	سلامه و همکاران، ۲۰۱۱
	حفاظت کامل از داده‌های مشتریان	ریزاردی، ۲۰۰۸
	ایجاد تیم‌های امنیتی متخصص در بانک‌ها	عثمان و شاه، ۲۰۱۳
	ایجاد نظام‌های کنترلی داخلی شدید در بانک‌ها	عثمان و شاه، ۲۰۱۳
	انجام خدمات مشتری به‌صورت واکنشی	عثمان و شاه، ۲۰۱۳
	انجام ممیزی‌های داخلی منظم	کرام، فرگوسن و مورونی، ۲۰۰۸

ادامهٔ جدول ۱

دسته‌بندی	عامل موفقیت	مرجع
عوامل فنی	تقویت سیستم‌های احراز هویت مشتریان با استفاده از عوامل بیومتریک	آکینیمی، اوموگبادگون و اویلامی، ۲۰۱۱
	رمزنگاری داده‌ها	گانسن، ۲۰۰۹
	مقیاس‌پذیر بودن سیستم‌های امنیتی	موسکویچ، ۲۰۰۹
	کاهش امکانات و اختیارات مدیریت سیستم	واندومل، ۲۰۱۰
	ارائهٔ راه حل‌های احراز هویت بادوام از نظر اقتصادی	موردوچ واندرسون، ۲۰۱۰
	کاربر دوست‌بودن (User friendliness) سیستم‌ها	واندومله، ۲۰۱۰
	تجمیع و یکپارچگی راه حل‌ها	عثمان و شاه، ۲۰۱۳

پس از شناسایی عوامل موفقیت مقابله با تقلب، اولویت‌بندی و رتبه‌بندی این عوامل می‌تواند گام مؤثری در تدوین استراتژی‌ها و روش‌های مقابله با تقلب باشد. متأسفانه در بررسی صورت‌گرفته تحقیقی که به رتبه‌بندی عوامل اشاره‌شده پرداخته باشد، مشاهده نشد (البته باید توجه شود اگر چنین تحقیقی در کشورهای دیگر نیز انجام شده باشد، با توجه به ویژگی‌های خاص ایران و تفاوت در زیرساخت‌های فرهنگی و تکنولوژی با سایر کشورها، لزوم چنین پژوهشی در داخل کشور نیز احساس می‌شود). بنابراین در تحقیق اخیر به‌منظور رفع این خلأ تحقیقاتی، نسبت به وزن‌دهی عوامل اشاره‌شده در بانکداری الکترونیک در کشور پرداخته خواهد شد.

روش شناسی پژوهش

مطالعهٔ پیش رو پژوهشی توصیفی ـ پیمایشی با ماهیت کاربردی است. این مطالعه در پی شناسایی و رتبه‌بندی عواملی است که بتوانند برای مقابله با تقلب‌های بانکداری الکترونیک، در بانک‌های کشور استفاده شوند. به این منظور، پژوهش حاضر در دو مرحله انجام می‌گیرد. در مرحلهٔ نخست عوامل مؤثر برای مقابله با تقلب در بانکداری الکترونیک با استفاده از مطالعات کتابخانه‌ای، مقالات و تحقیقات صورت‌گرفته تعیین می‌شوند. در مرحلهٔ دوم به‌کمک مدل فازی تصمیم‌گیری گروهی سلسله‌مراتبی، به رتبه‌بندی عوامل تعیین‌شده از طریق سؤالات پرسشنامه پرداخته خواهد شد.

با توجه به تخصصی بودن موضوع پژوهش، جامعهٔ آماری این تحقیق، خبرگان و کارشناسان فناوری اطلاعات شاغل در بانک‌های کشور در نظر گرفته شده است. به‌منظور تعیین اندازهٔ نمونهٔ (n) از رابطهٔ کوکران استفاده شد (کوکس و کوکران، ۱۹۵۳).

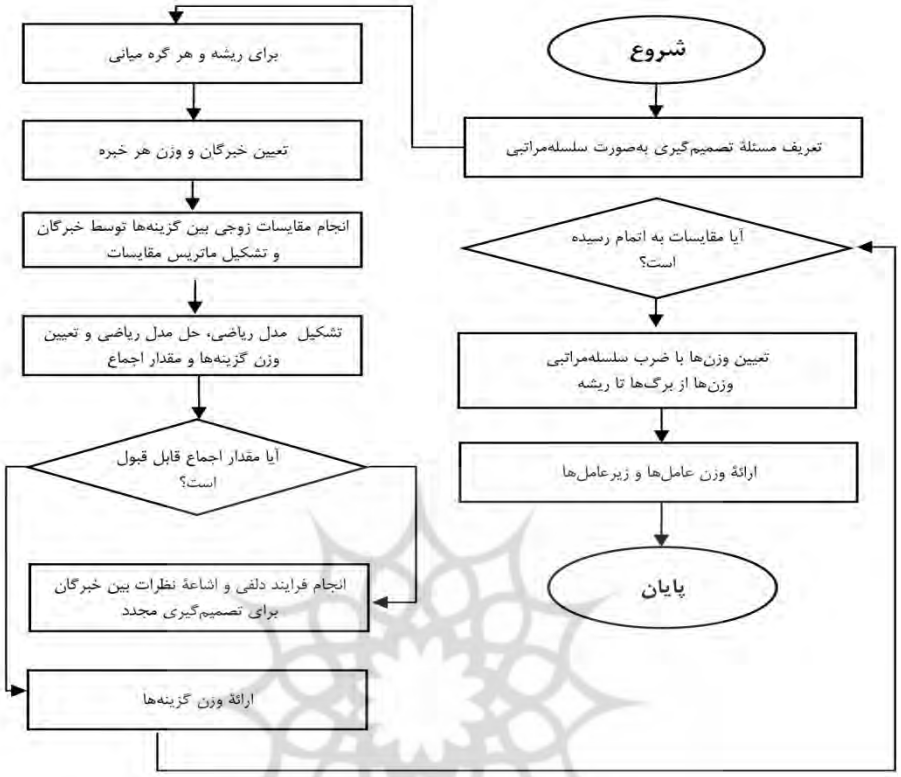
$$n = \frac{Nz^2p(1-p)}{Nd^2 + z^2p(1-p)}$$ رابطهٔ ۱)

که در آن N اندازهٔ جامعه، z مقدار خطای معیار ضریب اطمینان مورد قبول، p نسبت جمعیت بدون صفت خاص و d، دقت احتمالی مطلوب است.

با فرض بی‌نهایت بودن N، ضریب اطمینان ۹۰ درصدی (z =۱/۶۵)، بدبینانه‌ترین حالت برای p (p = ۰/۵) و دقت احتمالی ۰/۱ (d = ۰/۱)، حجم نمونه ۶۷ به‌دست آمد. پرسشنامهٔ تهیه‌شده برای ۷۲ نفر از متخصصان فناوری اطلاعات بانک‌ها و کارشناسان پلیس فضای تبادل اطلاعات (فتا) ارسال شد که از این تعداد ۷۰ پرسشنامه تکمیل شده و از اطلاعات ۶۹ پرسشنامه استفاده شد. تکمیل‌کنندگان پرسشنامهٔ تحقیق ۲۲ نفر از بانک اقتصاد نوین، ۱۵ نفر از بانک ملت، ۱۱ نفر از بانک مسکن، ۱۰ نفر از بانک ملی، ۷ نفر از بانک قرض‌الحسنهٔ مهر ایران و ۴ نفر از پلیس فتا بودند.

ابزار گردآوری داده‌ها: به‌منظور کسب نظر خبرگان در ماتریس مقایسات زوجی، از پرسشنامه استفاده شده است. پرسشنامه به‌گونه‌ای طراحی شده بود که به پاسخ‌دهندگان امکان مقایسهٔ زوجی معیارها و زیرمعیارها در گروه خود و تعیین اهمیت هر یک را می‌داد. برای سنجش روایی پرسشنامه‌ها، از نظر خبرگان فناوری اطلاعات، بانکداری الکترونیک و استادان دانشگاهی بهره برده شده است.

روش وزن‌دهی: روش وزن‌دهی معیارها در این تحقیق، مبتنی بر روش تصمیم‌گیری چندمعیارهٔ فازی میخایلوف (۲۰۰۴) است. در این روش، ابتدا تصمیم‌گیرندگان به مقایسهٔ زوجی گزینه‌ها می‌پردازند. پس از مقایسات زوجی، مدل میخایلوف (۲۰۰۴) استفاده می‌شود و چنانچه اجماع قابل قبولی وجود داشته باشد، وزن‌های ارائه‌شده توسط مدل پذیرفته می‌شود؛ در غیر این صورت با استفاده از مدل دلفی، نتایج برای تصمیم‌گیرندگان ارسال شده و از آنها درخواست می‌شود تا مقایسات خود را به‌هنگام کنند. در این روش برای هر تصمیم‌گیرنده، وزنی برای اهمیت تصمیم‌گیری اختصاص می‌یابد که عددی بین صفر و ۱ است، هرچه این عدد کوچک‌تر باشد، گویای اهمیت بیشتر تصمیمات فرد مد نظر خواهد بود. در انتها، وزن هر معیار از ضرب سلسله‌مراتبی وزن‌ها به‌دست می‌آید. شکل ۱ این فرایند را به نمایش گذاشته است.



شکل ۱. فرایند وزن‌دهی در تحقیق

تصمیم‌گیری گروهی فازی سلسله‌مراتبی برای وزن‌دهی

در فرایند تحلیل سلسله‌مراتبی (AHP) که به‌منظور تصمیم‌گیری چندمعیاره (فردی نه گروهی) توسعه یافته است، مقایسهٔ زوجی بین گزینه‌ها و معیارها به‌عنوان مبنای مدل ایفای نقش می‌کند (ساعتی، ۱۹۸۸). این مقایسه در قالب ماتریسی به‌صورت زیر نمایش داده می‌شود که در آن n تعداد گزینه‌های (یا معیارها) مقایسه‌شونده و a_{ij} معرف ارجحیت گزینهٔ i به گزینهٔ j از نظر فرد تصمیم‌گیرنده است.

$$A = \{a_{ij} | i = 1,2, \dots, n-1 , \quad j = 1,2, \dots, n\}$$

هدف AHP، نظیر هر تکنیک تصمیم‌گیری چندمعیارهٔ دیگر، یافتن وزن گزینه‌ها (معیارها) به‌صورت $W = (W_1, W_2, \dots, W_n)^T$ است که در آن W_k اهمیت گزینهٔ (یا معیار) i ام را نشان می‌دهد. در AHP سعی می‌شود، W_kها به‌گونه‌ای تعیین شوند که $\frac{W_i}{W_j}$ نزدیک به مقایسهٔ زوجی گزینهٔ i و j باشند. یا

$$\frac{W_i}{W_j} \approx a_{ij}$$ رابطهٔ ۲)

میخایلوف (۲۰۰۴) با توسعهٔ مدل AHP و با استفاده از نظریهٔ مجموعه‌های فازی، روشی برای تصمیم‌گیری گروهی ارائه کرد. در این روش برای تعیین مجموعهٔ وزن‌ها به‌صورت $W = (W_1, W_2, \dots, W_n)^T$ رابطهٔ ۳ جایگزین رابطهٔ ۲ می‌شود.

$$R_{ijk}(W) \cong 0$$ رابطهٔ ۳)

که در آن ≅ بیان‌کنندهٔ تساوی فازی است و $R_{ijk}(W)$ به‌صورت رابطهٔ ۴ تعریف می‌شود.

$$R_{ijk}(W) \cong W_i - a_{ijk}W_j$$ رابطهٔ ۴)

در رابطهٔ ۴، a_{ijk} بیان‌کنندهٔ مقایسهٔ گزینهٔ i ام با گزینهٔ j ام توسط فرد k ام است. میخایلوف (۲۰۰۴) مدل خود را بر اساس رابطهٔ ۴ توسعه داده است. در این روش با تعریف مفهومی به نام پارامتر انحرافی[1] (d_{ijk})، تابع عضویت[2] فازی به‌صورت رابطهٔ ۵ تعریف می‌شود.

$$\mu_{ijk}(W) = \begin{cases} 1 - \dfrac{R_{ijk}(W)}{d_{ijk}} & if \quad R_{ijk}(W) \geq 0 \\ 1 + \dfrac{R_{ijk}(W)}{d_{ijk}} & if \quad R_{ijk}(W) < 0 \end{cases}$$ رابطهٔ ۵)

پارامتر انحرافی (d_{ijk}) معرف انحراف فرد تصمیم‌گیرندهٔ k در تصمیم‌گیری در خصوص مقایسهٔ زوجی دو گزینهٔ i و j است. مقدار این پارامتر برای افراد مختلف و تصمیم‌های گوناگون، متفاوت است. هرچه این مقدار کمتر باشد، به این معناست که فرد قدرت تصمیم‌گیری بیشتری دارد و انحراف تصمیماتش کوچک‌تر است. چنانچه تمایزی بین افراد وجود نداشته باشد، می‌توان مقدار d_{ijk} را مساوی در نظر گرفت (معمولاً مقداری بین صفر و ۱) (میخایلوف، ۲۰۰۴).

برای فرد تصمیم‌گیرندهٔ k، برآورده شدن رابطهٔ ۴ اشتراکی از توابع عضویت رابطهٔ ۵ است که در یک فضای تصمیم n − ۱ بعدی به‌صورت رابطهٔ ۶ تعریف می‌شود.

$$Q^{n-1} = \{\mu_{ijk}(W) | i = 1, 2, \dots, n-1 \,;\, j = 2,3, \dots, n; j > i\}$$ رابطهٔ۶)

اشتراک توابع عضویت ذکرشده در فضای تعریف‌شده در رابطهٔ ۶ به‌صورت رابطهٔ ۷ است.

$$\mu_p(w) = \underset{p \epsilon Q^{n-1}}{\text{Min}} \{\mu_{ijk}(w) | i = 1, 2, \dots, n-1 \,;\, j = 2, 3, \dots, n \,;\, j > i\}$$ رابطهٔ ۷)

---

1. Deviational Parameter
2. Membership Function

در واقع، مدل به‌دنبال برداری در فضای تصمیم Q^{n-1} است که با توجه به درجات عضویت تمام افراد، دارای بزرگ‌ترین درجهٔ عضویت در تابع عضویت رابطهٔ ۷ باشد و یک بردار تصمیم نهایی بهینه با حداکثر رضایت گروهی به‌دست دهد (این درجه با λ نشان داده می‌شود).

رابطهٔ ۸) $$\lambda = \mathrm{Max}\left(\mu_p(w)\right) = \mathrm{Max}\left(\underset{w\epsilon Q^{n-1}}{\mathrm{Min}}\left[\mu_{ijk}(w)\right]\right)$$

رابطهٔ ۸ در قالب مدل بهینه‌سازی رابطهٔ ۹ قابل دستیابی است.

رابطهٔ ۹) $$Max\ \lambda$$

Subject to: $\lambda \leq \mu_{ijk}(w)$

مدل ارائه‌شده، نوعی مدل برنامه‌ریزی خطی است و مقدار λ بیشینهٔ حاصل از مدل، نشان‌دهندهٔ میزان اجماع تصمیم‌گیرندگان است. همان‌گونه که اشاره شد، λ مقداری بین صفر و ۱ است و هرچه به ۱ نزدیک‌تر باشد، گویای همگرایی بیشتر تصمیمات است (میخایلوف، ۲۰۰۴).

یافته‌های پژوهش

در این بخش، فرایند ارائه‌شده در شکل ۱ برای تعیین وزن عوامل مؤثر مقابله با تقلب در بانکداری الکترونیک طی خواهد شد و وزن معیارها بر این اساس تعیین می‌شود. حداقل مقدار اجماع که در این تحقیق در نظر گرفته شده، ۰/۷ است.

تعیین مسئلهٔ تصمیم‌گیری به‌صورت سلسله‌مراتبی: در گام نخست، عوامل مؤثر بر مقابله با تقلب در بانکداری الکترونیکی که از مرور ادبیات (جدول ۱) شناسایی شدند، به‌صورت سلسله‌مراتبی شکل می‌گیرند.

تعیین تصمیم‌گیرندگان و انحراف تصمیم‌گیری برای هر تصمیم‌گیرنده: تعداد خبرگان و افراد سهیم در تعیین وزن همان‌گونه که اشاره شد ۶۹ نفر است که انحراف تصمیم‌گیری برای تمام خبرگان و گزینه‌ها ۰/۵ فرض می‌شود.

انجام مقایسات زوجی بین عامل‌ها و زیرعامل‌ها توسط خبرگان: همان‌گونه که اشاره شد مقایسات زوجی بین عامل‌های مؤثر و زیرعامل‌ها (در مجموع ۵ ماتریس مقایسهٔ زوجی) توسط خبرگان در قالب پرسشنامه‌هایی صورت گرفت.

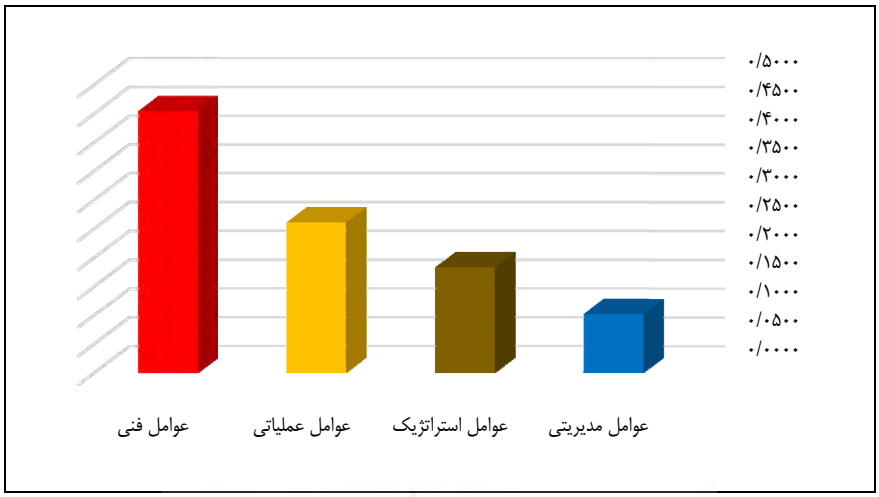
محاسبهٔ وزن‌ها با استفاده از مدل میخایلوف: با استفاده از ساختار سلسله‌مراتبی عامل‌ها، به‌منظور اطمینان از اجماع مد نظر، ابتدا مقدار اجماع به‌دست‌آمده در هر دسته از مقایسات زوجی (λ) در جدول ۲ درج شده است. جدول ۳ نیز وزن نهایی عامل‌ها و زیرعامل‌ها را نشان می‌دهد.

جدول ۲. مقدار اجماع گروهی در مقایسات زوجی عامل‌ها و زیرعامل‌ها

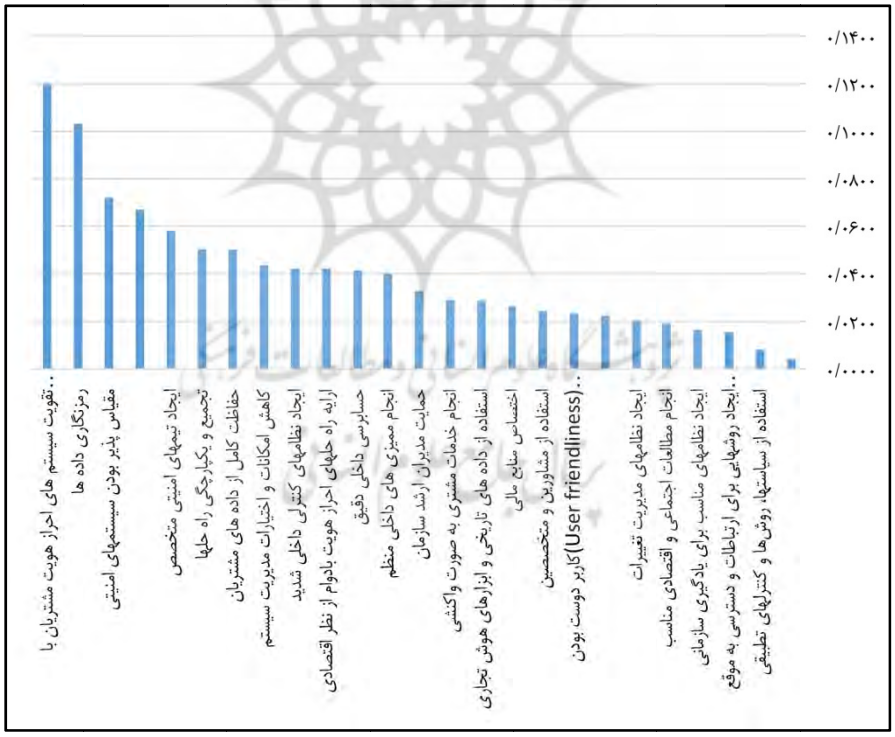
سطوح ساختار سلسله‌مراتب	عنوان ماتریس مقایسات زوجی	مقدار اجماع تصمیم‌گیری (λ)
سطح دوم	مقایسات زوجی عامل‌های مؤثر بر مقابله با تقلب	۰/۷۴
سطح سوم	مقایسات زوجی زیرعامل‌های استراتژیک	۰/۷۲
	مقایسات زوجی زیرعامل‌های مدیریتی	۰/۷۳
	مقایسات زوجی زیرعامل‌های عملیاتی	۰/۸۰
	مقایسات زوجی زیرعامل‌های فنی	۰/۸۲

جدول ۳. وزن عامل‌ها و زیرعامل‌ها

عوامل	وزن	زیرعامل	وزن محلی	وزن نهایی
عوامل استراتژیک	۰/۱۸۲۸	ایجاد روش‌هایی برای ارتباطات و دسترسی به‌موقع مدیران به اطلاعات	۰/۰۸۴۵	۰/۰۱۵۴
		ارائهٔ آموزش‌های کافی به کاربران خدمات بانکداری الکترونیک	۰/۳۶۶۰	۰/۰۶۶۹
		انجام مطالعات اجتماعی و اقتصادی مناسب	۰/۱۰۴۳	۰/۰۱۹۱
		استفاده از مشاوران و متخصصان	۰/۱۳۲۴	۰/۰۲۴۲
		ایجاد نظام‌های مناسب برای یادگیری سازمانی	۰/۰۹۰۷	۰/۰۱۶۶
		استفاده از سیاست‌ها، روش‌ها و کنترل‌های تطبیقی	۰/۰۴۳۸	۰/۰۰۸۰
		استفاده از اشخاص ثالث متخصص برای انجام معاملات آنلاین	۰/۰۲۱۹	۰/۰۰۴۰
		استفاده از داده‌های تاریخی و ابزارهای هوش تجاری	۰/۰۱۵۶۴	۰/۰۲۸۶
عوامل مدیریتی	۰/۱۰۱۸	اختصاص منابع مالی	۰/۲۵۹۵	۰/۰۲۶۴
		ایجاد آمادگی مدیران و کارکنان بانکی برای مقابله با تغییرات	۰/۲۲۰۴	۰/۰۲۲۴
		حمایت مدیران ارشد سازمان	۰/۳۲۱۶	۰/۰۳۲۷
		ایجاد نظام‌های مدیریت تغییرات	۰/۱۹۸۴	۰/۰۲۰۲
عوامل عملیاتی	۰/۲۶۰۹	حسابرسی داخلی دقیق	۰/۱۵۸۷	۰/۰۴۱۴
		حفاظت کامل از داده‌های مشتریان	۰/۱۹۲۱	۰/۰۵۰۱
		ایجاد تیم‌های امنیتی متخصص	۰/۲۲۲۴	۰/۰۵۸۰
		ایجاد نظام‌های کنترلی داخلی شدید	۰/۱۶۱۸	۰/۰۴۲۲
		انجام خدمات مشتری به‌صورت واکنشی	۰/۱۱۱۲	۰/۰۲۹۰
		انجام ممیزی‌های داخلی منظم	۰/۱۵۳۷	۰/۰۴۰۱
عوامل فنی	۰/۴۵۴۵	تقویت سیستم‌های احراز هویت مشتریان با استفاده از عوامل بیومتریک	۰/۲۶۳۴	۰/۱۱۹۷
		رمزنگاری داده‌ها	۰/۲۲۷۰	۰/۱۰۳۲
		مقیاس‌پذیر بودن سیستم‌های امنیتی	۰/۱۵۸۴	۰/۰۷۲۰
		کاهش امکانات و اختیارات مدیریت سیستم	۰/۰۹۵۹	۰/۰۴۳۶
		ارائهٔ راه حل‌های احراز هویت بادوام از نظر اقتصادی	۰/۰۹۲۸	۰/۰۴۲۲
		کاربر دوست‌بودن سیستم‌ها	۰/۰۵۱۵	۰/۰۲۳۴
		تجمیع و یکپارچگی راه حل‌ها	۰/۱۱۱۰	۰/۰۵۰۴



شکل ۲. وزن نهایی عوامل



شکل ۳. وزن نهایی زیرعامل‌ها

نتیجه‌گیری و پیشنهادها

مسائل امنیتی، مانع عمده‌ای در توسعهٔ بانکداری الکترونیکی و فعالیت‌های تجارت الکترونیک میان مصرف‌کنندگان است (خساونه، الاعظم و بسول، ۲۰۰۹). در تحقیقات پیشین، مسئلهٔ تقلب خطر مهمی برای سیستم‌های پرداخت شناخته شده است (شاه، ۲۰۱۶). برای تأمین امنیت سیستم بانکداری الکترونیکی، تأکید محققان بر تعریف اهداف روشن است. این موضوع که با درک اهداف کسب‌وکار، عوامل موفقیت هنگام برنامه‌ریزی استراتژیک امنیت مدنظر قرار گیرد و تأثیر این عوامل بر کسب‌وکار تعیین شود، امری حیاتی در توسعهٔ روش‌های مقابله با تقلب در این عرصه است (کیلی، ۲۰۰۱).

در این مقاله به بررسی و شناسایی عوامل موفقیت مقابله با تقلب پرداخته شد و تعداد ۲۵ عامل در چهار دستهٔ عوامل استراتژیک، مدیریتی، عملیاتی و فنی شناسایی شدند؛ سپس با بهره‌مندی از تصمیم‌گیری گروهی به وزن‌دهی عوامل شناسایی‌شده پرداخته شد و وزن هر عامل و زیرعامل به‌دست آمد. این پژوهش، نخستین مطالعه‌ای است که در کشور به اولویت‌بندی عوامل موفقیت در مقابله با تقلب پرداخته است و از این جنبه امکان مقایسهٔ خروجی‌های تحقیق با تحقیقات پیشین وجود ندارد.

همان‌گونه که انتظار می‌رود نتیجهٔ تحقیق گویای اهمیت بیشتر عوامل فنی نسبت به سایر عوامل در مقابله با تقلب است. این امر با تحقیقات پیشین در این حوزه همخوانی دارد (عثمان و شاه، ۲۰۱۳). البته باید توجه داشت که از نظر خبرگان تحقیق، عوامل غیرفنی در مجموع بیش از ۵۵ درصد اهمیت وزنی را در مقابله با تقلب دارند و این نشان می‌دهد پرداختن صرف به عوامل فنی برای مقابله با تقلب کارساز نخواهد بود (فاطیما، ۲۰۱۱). بر اساس یافته‌های تحقیق، پس از عوامل فنی، عوامل عملیاتی، استراتژیک و مدیریتی به‌ترتیب در رده‌های بعدی اهمیت قرار دارند.

در بررسی زیرعامل‌ها، سه عامل فنی تقویت سیستم‌های احراز هویت، رمزنگاری داده‌ها و مقیاس‌پذیری سیستم‌های امنیت، از دید خبرگان و بر اساس نتایج تصمیم‌گیری گروهی اهمیت بیشتری داشتند. این نتیجه در واقع تأییدی بر تحقیقات صورت‌گرفته نظیر عثمان و شاه (۲۰۱۳)، روبردرز (۱۹۹۸)، باتاچارایا و همکاران (۲۰۰۹)، اکینیمی و همکاران (۲۰۱۱) است. این محققان نیز نشان دادند که برای مقابله با تقلب، باید در طراحی سیستم‌های بانکداری الکترونیکی مباحث امنیتی در کانون توجه قرار گیرند.

زیرعامل دیگری که در اولویت بعدی قرار دارد و از دستهٔ عوامل استراتژیک است، ارائهٔ آموزش‌های کافی به کاربران در خصوص خدمات بانکداری الکترونیک است. در طراحی خدمات بانکداری، لازم است به مشتریان برای محافظت از اطلاعات شخصی آموزش‌های کافی داده

شود تا متقلبان نتوانند از طریق اقدامات متقلبانه نظیر فیشینگ به این اطلاعات دسترسی پیدا کنند (ریزاردی، ۲۰۰۸).

زیرعامل غیرفنی دیگری که از نظر خبرگان با اهمیت تشخیص داده شد، استقرار تیم‌های امنیتی در بانک‌ها برای مقابله با تقلب است. واقعیت این است که هرچند بانک‌ها هر روز سیستم‌های خود را از نظر امنیتی ارتقا می‌دهند، اعمال متقلبانه نیز به مرور زمان پیچیده‌تر می‌شوند و هر لحظه امکان حملهٔ جدید امنیتی برای تقلب به سیستم‌های بانکی وجود دارد. بنابراین لازم است تیم‌های تخصصی امنیتی در بانک‌ها تشکیل شوند تا ضمن شناسایی اعمال متقلبانهٔ جدید، با واکنش سریع نسبت به رفع مشکلات امنیتی سیستم‌های بانکی اقدام کنند (عثمان و شاه، ۲۰۱۳). پژوهش حاضر همچنین بر اهمیت حفاظت از داده‌های مشتریان توسط کارکنان بانکی تأکید دارد و این تأییدی بر یافته‌های ریزاردی (۲۰۰۸) در این زمینه است.

نتایج پژوهش اهمیت یکپارچه‌سازی خدمات بانکداری و تجمیع راه حل‌ها را برای مقابله با تقلب بیان می‌کند. در توجیه این مسئله می‌توان گفت که با تجمیع خدمات بانکداری، تیم‌های عملیاتی و امنیتی بر سیستم‌های مختلف تمرکز نخواهند داشت. از این رو امکان حل مشکلات امنیتی بیش از پیش فراهم خواهد شد. به‌علاوه با تجمیع راه حل‌ها، عملاً نظام‌های امنیتی نیز یکپارچه شده و در صورت شناسایی و رفع خطای امنیتی در بخشی از سیستم، این خطا در سایر خدمات بانکداری الکترونیک نیز رفع خواهد شد (عثمان و شاه، ۲۰۱۳).

همان‌گونه که پیشتر نیز اشاره شد، در این تحقیق با مرور ادبیات، عوامل موفقیت مقابله با تقلب در بانکداری الکترونیک شناسایی شد و اولویت‌بندی این عوامل با نظر خبرگان حوزهٔ بانکداری الکترونیک صورت گرفت. استفاده از روش‌های تجربی برای شناسایی عوامل موفقیت مقابله با تقلب (بررسی تراکنش‌ها و تقلب‌های صورت گرفتهٔ پیشین در کشور و استخراج آنها از طریق روش‌هایی مانند داده‌کاوی که مبتنی بر دادهٔ واقعی و تجربه‌های گذشته است) یکی از زمینه‌های تحقیقاتی است که به محققان پیشنهاد می‌شود.

همچنین بر اساس نتایج پژوهش، عامل تقویت سیستم‌های احراز هویت به‌عنوان مهم‌ترین عامل برای مقابله با تقلب شناسایی شد. به‌طبع، بهره‌مندی از روش‌های جدیدتر احراز هویت، نظیر بیومتریک‌ها به تدوین قوانین و مقررات جدیدی در حوزهٔ معاملات بانکداری الکترونیک نیاز دارد که این موضوع می‌تواند به‌عنوان پژوهشی کاربردی برای تحقیقات آتی، در کانون توجه قرار گیرد.

بهره‌مندی از عوامل شناسایی‌شده در طراحی سیستم‌های اطلاعاتی و راهکارهای سازمانی، استراتژیک و مدیریتی، موضوعات دیگری هستند که برای تحقیقات آتی پیشنهاد می‌شود.

پژوهش دیگری که می‌تواند در راستای تحقیق حاضر اجرا شود، بررسی وضعیت موجود خدمات الکترونیک در کشور از بعد فنی و غیرفنی بر اساس عوامل شناسایی‌شده در این مقاله است.

منابع

پوررضا، م. (۱۳۹۴). سیر تحول جرایم سایبری و راهکارهای مقابله با آن در حقوق ایران، *کنفرانس ملی هزارهٔ سوم و علوم انسانی*، شیراز، ایران.

تقوا، م.؛ منصوری، ط.؛ فیضی، ک. و اخگر، ب. (۱۳۹۵). کشف تقلب در تراکنش‌های کارت‌های بانکی با استفاده از پردازش موازی ناهنجاری در بزرگ‌داده، *فصلنامهٔ علمی ـ پژوهشی مدیریت فناوری اطلاعات*، ۸ (۳)، ۴۹۸- ۴۷۷.

دامغانیان، ح. و کجوری، م.، س. (۱۳۹۱). بررسی تأثیر امنیت ادراک‌شده بر اعتماد به بانکداری اینترنتی از سوی مشتریان زن (پیمایشی دربارهٔ بانک صادرات شهر سمنان)، *فصلنامهٔ علمی ـ پژوهشی مدیریت فناوری اطلاعات*، ۴ (۱۳)، ۸۸-۷۱.

راسخی، ا. (۱۳۹۳). جرائم و تهدیدهای سایبری و نقش پلیس در توسعه امنیت نرم در محیط سایبر. *فصلنامهٔ مطالعات حفاظت و امنیت انتظامی*، ۳۲(۳)، ۲۰۱-۲۵۲.

محقر، ع.؛ لوکس، ک.؛ حسینی، ف. و منشی آ. ع. (۱۳۸۷). کاربرد هوش تجاری به‌عنوان یک تکنولوژی اطلاعات استراتژیک در بانکداری: بازرسی و کشف تقلب. *فصلنامهٔ علمی ـ پژوهشی مدیریت فناوری اطلاعات*، ۱(۱)، ۱۲۰- ۱۰۵.

موسوی، پ.؛ زنوز، ر.ی. و حسن‌پور، ا. (۱۳۹۴). شناسایی ریسک‌های امنیت اطلاعات سازمانی با استفاده از روش دلفی فازی در صنعت بانکداری. *فصلنامهٔ علمی ـ پژوهشی مدیریت فناوری اطلاعات*، ۷ (۱)، ۱۸۴- ۱۶۳.

وثوق، م.؛ تقوی‌فرد، م. ت و البرزی، م. (۱۳۹۳) شناسایی تقلب در کارت‌های بانکی با استفاده از شبکه‌های عصبی مصنوعی، *فصلنامهٔ علمی ـ پژوهشی مدیریت فناوری اطلاعات*، ۶ (۴)، ۷۴۶- ۷۲۱.

Abreu, R., Segura, L., David, F., Formigoni, H., Legčević, J. & Mantovani, F. (2015). Ethics and fraud in E-banking services. *Information Systems and Technologies (CISTI), 2015 10th Iberian Conference on* (pp. 1-6). IEEE.

AbuAli, A.N. & Abu-Addose, H.Y. (2010). Data warehouse critical success factors. *European Journal of Scientific Research*, 42(2), 326-335.

Abubakre, M., Coombs, C., Jayawardhena, C. & Hunt, A. (2010). Learning the Lessons from the Developed World: e-Banking Security in Nigeria. *Learning*, 3(1), 1-23.

Adams, R. (2010). Prevent, protect, pursue–a paradigm for preventing fraud. *Computer Fraud & Security*, 2010 (7), 5-11.

Akinyemi, O., Omogbadegun, Z.O. & Oyelami, O.M. (2011). Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-Banking System. *International Journal of Electrical & Computer Sciences*, 10(6).

Albrecht, W.S., Albrecht, C & Albrecht, C.C. (2008). Current trends in fraud and its detection. *Information Security Journal: A Global Perspective*, 17(1), 2-12.

Auta, E.M. (2010). E-banking in developing economy: Empirical evidence from Nigeria. *Journal of applied quantitative methods*, 5(2), 212-222.

Benjamin, O.A. & Samson, B.S. (2011). Effect of perceived inequality and perceived job insecurity on fraudulent intent of bank employees in Nigeria. *Europe's Journal of Psychology*, *7*(1), 99-111.

Bhattacharyya, D., Ranjan, R., Alisherov F. A. & Choi, M. (2009). Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology*, 2(3), 13-28.

Button, M. & Gee, J. (2013). *Countering fraud for competitive advantage: the professional approach to reducing the last great hidden cost*. United Kingdom: John Wiley & Sons.

Choplin, J.M., Stark, D.P. & Ahmad, J.N. (2011). A Psychological Investigation of Consumer Vulnerability to Fraud: Legal and Policy Implication. *The Law & Psychology Review*, 35, P. 61.

Coram, P., Ferguson, C. & Moroney, R. (2008). Internal audit, alternative internal audit structures and the level of misappropriation of assets fraud. *Accounting & Finance*, 48(4), 543-559.

Cox, G.M. & Cochran, W.G. (1953). *Experimental designs*. NewJersey: Wiley.

Damghanian, H. & Kojouri, M. S. (2013). A Study on the Effect of Perceived Security on the Trust of Female Customers in the Internet Banking: (A Survey of the SADERAT BANK in Semnan). *Journal of Information Technology Management*, 4(13), 71-88 (*in Persian*).

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. *Risk Governance and Control: Financial Markets and Institutions*, *4*(2), 16-26.

Falzon, J. & Gardener, E. (2016). *Strategic challenges in European banking*. Berlin: Springer.

Fatima, A. (2011). E-Banking Security issues-Is there a solution in biometrics? *Journal of Internet Banking and Commerce*, 16(2), 1-15.

Fedrizzi, M., Molinari, A. & Ventre, V. (2004). A model for evaluating the transaction risk in e-banking. *IADIS International Conference e-Society Avila*, 7(1), 172-178.

Ganesan, R. (2009). A secured hybrid architecture model for internet banking (e-banking). *Journal of Internet Banking and Commerce*, 14(1), 1-17.

Giles, J. (2010). The problem with online banking. *New Scientist*, 205 (2745), 18-19.

Igwe, C.N. (2011). Socio-economic developments and the rise of 419 advanced-fee fraud in Nigeria. *European Journal of Social Science*, 20(1), 184-193.

Johnson, M. & Moore, S. (2007), October. A new approach to e-banking. *Proc. 12th Nordic Workshop on Secure IT Systems (NORDSEC 2007)*, PP. 127-138.

Keely, D. (2001). A security strategy for mobile e-business, NewYork: IBM.

Khasawneh, A., Al Azzam, I. & Bsoul, M. (2009). A study on e-commerce security in Jordan. *International Journal of Electronic Finance*, 3(2), 166-176.

Koskosas, I. (2011). E-banking security: A communication perspective. *Risk Management*, 13(1), 81-99.

Leukfeldt, E.R., Kleemans, E.R. & Stol, W.P. (2016). Cybercriminal Networks, Social Ties and Online Forums: Social Ties versus Digital Ties within Phishing and Malware Networks. *British Journal of Criminology*, 57 (3), 704-722.

Liébana-Cabanillas, F., Muñoz-Leiva, F., Sánchez-Fernández, J. & Viedma-del Jesús, M.I. (2016). The moderating effect of user experience on satisfaction with electronic banking: empirical evidence from the Spanish case. *Information Systems and e-Business Management*, *14*(1), 141-165.

Mathivanan, B. & Kavitha, S. (2015). A Study on Consumer Perception towards E-Banking Services of ICICI Bank. *International Journal of Innovative Research and Development*, 4(12), 26-33.

Mikhailov, L. (2004). Group prioritization in the AHP by fuzzy preference programming method. *Computers & operations research*, 31(2), 293-301.

Mohaghar, A., Lucas, C., Hoseini, F., Monshi, A. (2009). Use of Business Intelligence as a Strategic Information Technology in Banking: Farud Discovery & Detection, *Journal of Information Technology Management*, 1(1), 105-120. (*in Persian*)

Montazemi, A.R. & Qahri-Saremi, H. (2015). Factors affecting adoption of online banking: A meta-analytic structural equation modeling study. *Information & Management*, 52(2), 210-226.

Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafić, T., Camtepe, A., Löhlein, B., Heister, U., Möller, S., Rokach, L. & Elovici, Y. (2009). Identity theft, computers and behavioral biometrics. *Intelligence and Security Informatics, 2009. ISI'09. IEEE International Conference on* (pp. 155-160). IEEE.

Mousavi, P., Zonouz, R. Y. & Hasanpour, A. (2014). Identifying Organizational Information Security Risks Using Fuzzy Delphi. *Journal of Information Technology Management*, 7(1), 163-184. (*in Persian*)

Murdoch, S.J. & Anderson, R. (2010). Verified by visa and MasterCard secure code: or, how not to design authentication. In *Financial Cryptography and Data Security*. Springer Berlin Heidelberg.

Okpara, G.C. (2009). A synthesis of the critical factors affecting performance of the Nigerian banking system. *European Journal of Economics, Finance and Administrative Sciences*, *17*, 34-44.

Ong, C.S. & Lin, Y.L. (2015). Security, risk and trust in individual internet banking adoption: an integrated model. *International Journal of Electronic Commerce Studies*, *6*(2), 343.

Parameswar, N., Dhir, S. & Dhir, S. (2017). Banking on Innovation, Innovation in Banking at ICICI Bank. *Global Business and Organizational Excellence*, *36*(2), 6-16.

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H. & Pahnila, S. (2004). Consumer acceptance of online banking: an extension of the technology acceptance model. *Internet research*, 14(3), 224-235.

Pourreza, M. (2015). The evolution of cybercrime and the ways of dealing with the rights of Iran. *National Conference on the Third Millennium and Humanities*, Shiraz. (*in Persian*)

Rana, P. J. & Baria, J. (2015). A Survey on Fraud Detection Techniques in Ecommerce. *International Journal of Computer Applications*, 113(14), 5-7.

Rasekhi, A. (2014). Crime and cyber threats and the role of police in the development of soft security in cyberspace. *Quarterly studies on security and protection*, 32, 201-252. (*in Persian*)

Rizzardi, R. (2008). Financial Management-Payment Card Fraud Can Happen to You. *Optometry and vision development*, *39*(2), 64.

Roberds, W. (1998). The impact of fraud on new methods of retail payment. *Economic Review-Federal Reserve Bank of Atlanta*, 83(1), 42-52.

Saaty, T. L. (1988). What is the analytic hierarchy process?. In *Mathematical models for decision support*. Springer Berlin Heidelberg.

Salameh, R., Al-Weshah, G., Al-Nsour, M. & Al-Hiyari, A. (2011). Alternative Internal Audit Structures and Perceived Effectiveness of Internal Audit in Fraud Prevention: Evidence from Jordanian Banking Industry. *Canadian Social Science*, 7(3), 40-50.

Salehi, M. & Alipour, M. (2010). E-banking in emerging economy: empirical evidence of Iran. *International Journal of Economics and Finance*, *2*(1), 201-209.

Sathye, M. (1999). Adoption of Internet banking by Australian consumers: an empirical investigation. *International Journal of bank marketing*, 17(7), 324-334.

Saxena, M.D. & Agrawal, R. (2016). Review of the Literature on Adoption and Use of Electronic Banking Channels Over Last Three Decades. *Imperial Journal of Interdisciplinary Research*, *2*(8), 1556-1569.

Shah, K.K. (2016). Electronic Banking: Its Use and Challenge in Nepal. *Academic Voices: A Multidisciplinary Journal*, 5, 9-15.

Simon, S.J., 2004. Critical success factors for electronic services: Challenges for developing countries. *Journal of Global Information Technology Management, 7*(2), 31-53.

Sun, Y. & Davidson, I. (2015). Influential factors of online fraud occurrence in retailing banking sectors from a global prospective: An empirical study of individual customers in the UK and China. *Information & Computer Security*, *23*(1), 3-19.

Taghva, M., Mansouri, T., Feizi, K. & Akhgar, B. (2016). Fraud Detection in Credit Card Transactions; Using Parallel Processing of Anomalies in Big Data, *Journal of Information Technology Management*, 8(3), 477-498. (*in Persian*)

Tan, J.J., Titkov, L. & Poslad, S. (2002). Securing agent-based e-banking services. In *Trust, Reputation, and Security: Theories and Practice*. Springer Berlin Heidelberg.

Usman, A. K. & Shah M. H. 2013. Critical Success Factors for Preventing e-Banking Fraud. *Journal of Internet Banking and Commerce*, 18(2), 1-14.

Vandommele, T. (2010). Biometric authentication today. *Proceedings of the Seminar on Network Security*. Available in: http://www.cse.hut.fi/en/publications/B/11/papers/vandommele.pdf.

Vosough, M., Taghavifard, M. T & Alborzi M. (2015). Bank card fraud detection using artificial neural network. *Journal of Information Technology Management*, 6(4), 721-746. (*in Persian*)