

بررسی عوامل موثر بر تمایل کاربران شعب بانک کشاورزی بر پذیرش اینترنت اشیا از دیدگاه امنیت

محمد ملکی نیا^۱، میثم سپهر کیا^۲

^۱ استادیار گروه مدیریت فناوری اطلاعات، دانشکده مدیریت، بین الملل کیش، دانشگاه آزاد، کیش، ایران.
^۲ دانشجوی دکتری مدیریت فناوری اطلاعات، دانشکده مدیریت، بین الملل کیش، دانشگاه آزاد، کیش، ایران.

نام نویسنده مسئول:

محمد ملکی نیا

تاریخ دریافت: ۱۴۰۰/۰۷/۱۵

تاریخ پذیرش: ۱۴۰۰/۰۹/۱۳

چکیده

زمینه و هدف: با گسترش روزافزون اینترنت و افزایش حسگرها و ابزارهای هوشمند در دسترس، اکنون شاهد شکل نوین استفاده از اینترنت هستیم که با عنوان اینترنت اشیا *IOT* شناخته می شود. برنامه های کاربردی اینترنت اشیا می توانند بین انسان ها، بین انسان ها و اشیا، بین اشیا و اشیا توسعه پیدا کنند. در واقع اینترنت اشیا یک پارادایم جدید است که ایده اولیه آن براساس تعامل مستمر انواع چیزهایی که در اطراف ما هستند ایجاد شده است. این تعامل مستمر باعث به خطر افتادن امنیت اطلاعات و حریم خصوصی افراد گردیده، زیرا سازوکار موثری برای شخصی سازی حریم خصوصی در این پارادایم، پیاده سازی نشده است. هدف اصلی این پژوهش، بررسی تاثیر نگرش و تمایل نسبت به استفاده از ابزارهای دیجیتالی در صنعت بانکداری الکترونیکی می باشد که به آزمون ۵ مولفه اصلی می پردازد، پژوهش حاضر از نظر روش و ماهیت، از جمله تحقیقات علی است، و به لحاظ اجرا پیمایشی و از نظر هدف کاربردی بوده و از مدل *TAM* برای بررسی ارتباط بین اجزای مدل بهره برده است. روش پیشنهاد شده از دو منبع اصلی ساخته شده: اول مرور ادبیات و دوم از طریق برداشت های حاصل از یک نظرسنجی غیر رسمی و مصاحبه با پنجاه نفر از کاربران بانک کشاورزی از طریق پرسشنامه و همچنین مصاحبه با شش نفر از خبرگان. نتایج حاصل از پژوهش گویای این مساله است که بخش بانکی برای نوآوری های اینترنت اشیا و تبدیل سایت های شعب سنتی بانک کشاورزی به محیط های هوشمند آماده است. ماهیت آزمایشی این یافته ها توجیه کافی برای آزمایش اینترنت اشیا برای امنیت فیزیکی بانکی با معرفی یک سیستم حفاظت هوشمند برای مدیریت فرایندهای امنیت را دارد. بررسی مقالات و کمبود مطالعات موجود ما را تشویق می کند تا استفاده از اینترنت اشیا برای امنیت اطلاعات مشتریان بانک را به طور گسترده تری بررسی کنیم.

واژگان کلیدی: بانک کشاورزی، پذیرش اینترنت اشیا، امنیت، ابزارهای دیجیتالی، هوشمند سازی خدمات

مقدمه

اینترنت به عنوان یک ابزار چند رسانه ای و نوین ارتباطی و اطلاع رسانی در عمر کوتاه خود به سرعت در میان اقشار مختلف جوامع نفوذ کرده است و به مکانی برای حضور شرکت ها و سازمان های مختلف تبدیل شده است. در این میان، یکی از بزرگ ترین فرصت ها و چالش هایی که سازمان های امروزی با آن مواجه هستند استفاده از اینترنت اشیاء است. میزان مبادلات از طریق اینترنت روز به روز افزایش یافته و شرکت هایی که از این فناوری استفاده نکنند ظرف مدت کوتاهی از صحنه بازار محو خواهند شد (کولپاس و همکاران، ۲۰۱۷). لذا برای رقابت و کسب مزیت، بانک ها مجبور هستند جدیدترین خدماتی را که مشتریان خواستار آن هستند در اختیارشان قرار دهند. در این راستا بانک کشاورزی همچون بانک های بسیاری در سطح جهان به ارائه خدمات اینترنت اشیاء پرداخته است، زیرا میدانند که اصل بقای آنها سرعت در ارائه خدمات اینترنت اشیاء و اطلاع رسانی در این زمینه به مشتریان است انتظار می رود بازار خدمات اینترنت اشیاء به یکی از مهم ترین حوزه ها جهت رقابت بانک ها و مؤسسات مالی با یکدیگر تبدیل شود (ژو و همکاران، ۲۰۲۱).

با توسعه فن آوری اطلاعات و ارتباطات و رشد روز افزون معاملات و تجارت الکترونیک در سطح جهان و نیاز تجارت الکترونیک به حضور بانک جهت نقل و انتقال منابع مالی، به جرات می توان گفت بدون خدمات اینترنت اشیاء، تجارت الکترونیکی اثربخش نیز محقق نخواهد شد لذا عواملی که بر پذیرش خدمات اینترنت اشیاء تاثیر می گذارد بسیار حائز اهمیت می باشد.

اینترنت اشیاء در بازه زمانی سال های ۲۰۰۸ و ۲۰۰۹ متولد شده است و پیش بینی می شود تعداد ابزارهای متصل در سال ۲۰۲۰ به ۵۰ میلیارد برسد. (ایوانس ۲۰۱۱). هدف اینترنت اشیاء توانمند سازی اشیاء برای اتصال در هر زمان و مکان، با هر چیزی و هر شخصی است که از هر مسیر یا شبکه و خدمت به صورت ایده آل استفاده می کند. اینترنت اشیاء تکامل جدیدی از اینترنت است. اینترنت اشیاء فناوری جدیدی است که به حضور نافذ محیطی توجه می کند و از تنوع چیزهایی با اتصالات بی سیم و سیم دار به محاوره با یکدیگر می پردازد. این اشیاء برای ایجاد کاربردها یا خدمات جدید و دستیابی به اهداف مشترک با یکدیگر همکاری می کنند و در واقع چالش های توسعه برای ایجاد جهانی هوشمند و بزرگ به شمار می روند. اکنون اینترنت اشیاء از دوران کودکی خارج شده و کاربردها و خدمات متنوع نوآورانه ای را برای کسب و کارها، افراد و دولت ها، فراهم کرده است. از این رو پژوهشگران و سازمان های پژوهشی بین المللی آن را انقلاب بعدی فناوری اطلاعات و ارتباطات معرفی کرده اند (قاسمی و همکاران، ۱۳۹۵).

باید توجه داشت که استفاده از فن آوری اطلاعات در عرصه بانکداری توانسته است علاوه بر ارائه ارزش و مزیت های متعددی همچون کاهش هزینه های مالی و زمانی و ارائه خدمات نوین به مشتریان در قالب خدماتی همچون بانکداری الکترونیک و موبایل بانک، بسیاری از فعالیت ها و فرایندهای غیرضروری در فرایند خدمت رسانی به مشتریان را حذف کند. با این وجود یکی از چالش های مهمی که بر سر راه کاربرد این فناوری ها و خدمات به مشتریان وجود دارد مساله امنیت اطلاعات مشتریان است. به عبارت دیگر این فناوری همانند سایر فناوری ها همچون سکه دو رو دارد اگر به همان اندازه که به توسعه و ترویج آن توجه می شود به امنیت آن توجه نشود می تواند به یک تهدید و چالش بزرگ تبدیل شود (الفت و همکاران، ۱۳۹۹). در حال حاضر وضعیت امنیت اطلاعات بانک ها در کشور بویژه در بانک های دولتی در سطح چندان مطلوبی نمی باشد، از جمله دلایل اصلی این وضعیت می توان زیرساخت های فنی و اجرایی امنیت و عدم انجام اقدامات موثر در خصوص ایمن سازی فضای تبادل اطلاعات دانست، بنابر این با توجه به صنعت بانکداری و خدماتی مثل موبایل بانک و بانکداری الکترونیک در صورت ضعف مدیریت امنیت اطلاعات می تواند به پیامدهای نامطلوبی همچون عدم اعتماد مشتریان، هک شدن حساب های مشتریان، کاهش وجهه بانک نزد جامعه، کاهش سپرده گذاری مشتریان و سرانجام افت عملکرد بانک منجر شود (اسدزاد، ۱۴۰۰). در چنین شرایطی توجه به مکانیزم های امنیتی، اهمیت ویژه ای یافته است و نگرانی های زیادی برای به خطر افتادن حریم خصوصی به وجود آمده، تا آنجایی که به عقیده بسیاری از پژوهشگران موفقیت و رشد بیشتر اینترنت اشیاء در آینده در گرو رفع این نگرانی ها می باشد. (محمد جمالو و همکاران ۱۳۹۷).

مروری بر ادبیات علمی تحقیق

با گسترش روزافزون اینترنت و افزایش حسگرها و ابزارهای هوشمند در دسترس، اکنون شاهد شکل نوین استفاده از اینترنت هستیم که با عنوان اینترنت اشیا^۱ IOT شناخته می‌شود. اینترنت اشیا محیطی را ایجاد می‌کند که در آن تعدادی حسگر و عملگر با قابلیت پایش از راه دور، می‌تواند به هر تخصصی یاری رساند. در این فضای جدید، دستگاه‌های پوشیدنی با قابلیت دریافت اطلاعات افراد، روز به روز محبوبیت بیشتری بین کاربران پیدا کرده‌اند و می‌توانند میزان تحرک افراد، ضربان قلب و بسیاری از فعالیت‌های دیگر آنها را اندازه‌گیری و برای مراکز تعیین شده مخابره نمایند. (وحدت، ۲۰۱۷).

اینترنت اشیا (IOT) مفهوم نوظهوری است که همگام با توسعه فناوری‌های مربوط به طراحی و ساخت حسگرها و همچنین فناوری‌های ارتباطی و اطلاعاتی گسترش یافت. تعاریف مختلفی از دیدگاه‌های متفاوتی وجود دارد. تعریف مرجع در این پژوهش، توسط اتحادیه ارتباطات بین‌المللی ارائه شده است. مطابق این تعریف، اینترنت اشیا زیرساختی جهانی برای جامعه اطلاعاتی معرفی می‌شود که سرویس‌های پیشرفته را از طریق ارتباطات داخلی بین اشیا و بر مبنای فناوری‌های ارتباطی و اطلاعاتی همکنش پذیر^۲ فراهم می‌آورد. در این تعریف شی به عنوان نمونه‌ای قابل شناسایی و منحصر بفرد از جهان فیزیکی و یا دنیای اطلاعاتی در نظر گرفته می‌شود که می‌تواند با شبکه ارتباطاتی تلفیق شود. IOT به علت وب مبنا و آنی بودن، توانایی دسترسی به شبکه وسیعی از اشیا و نیز فراهم آوردن بستری جهت همکاری‌های ملی و بین‌المللی، به هیچ‌مرز فیزیکی محدود نبوده و در بسیاری از حوزه‌ها، کاربردی است (حبیبی و آل شیخ، ۱۳۹۶).

فناوری اینترنت اشیا به سرعت در حال رشد است و پیش‌بینی می‌شود که در آینده یکی از مهم‌ترین عوامل تاثیرگذار در منطق کسب و کار و نیز در تمام صنایع باشد. اینترنت اشیا، منجر به افزایش کارایی و دقت، توأم با سود اقتصادی بیشتر و کاهش مداخلات انسانی می‌شود. برنامه‌های کاربردی اینترنت اشیا می‌توانند بین انسان‌ها، بین انسان‌ها و اشیا، بین اشیا و اشیا توسعه پیدا کنند.

از نقطه نظر مفهومی، فناوری اینترنتی از اشیا بر اساس سه اصل حیاتی که به هوشمندسازی اشیا مربوط می‌شود، بنا شده است: (۱) قابلیت شناسایی خودکار اشیا هوشمند، (۲) قابلیت ارتباط اشیا هوشمند با محیط اطرافشان، و (۳) قابلیت برقراری تعامل میان خود اشیا در شبکه اصلی تشکیل دهنده آن‌ها و نیز ارسال اطلاعات مورد نیاز به استفاده‌کنندگان (بانک‌ها، کاربران نهایی و سازمانهای خدماتی، دولت و... (چن و ژین، ۲۰۱۸).

بسیاری از کارهای تحقیقاتی برای ارائه نظریه‌ها و مدل‌ها برای بررسی عواملی که بر قصد رفتاری کاربران برای اتخاذ یک سیستم جدید تاثیر دارند، وجود دارد. (راجرز، ۱۹۶۲)

در میان این مدل‌ها و نظریه‌های ارائه شده، (TAM پیشنهادی دیویس، ۱۹۸۹) به طور گسترده‌ای برای تفسیر الگوی رفتاری کاربر برای پذیرش نوآوری مورد استفاده قرار می‌گیرد زیرا از روانشناسی اجتماعی کمک گرفته است.

بسیاری از محققان عقیده دارند که سازه‌های ارائه شده توسط TAM برای بررسی الگوی رفتاری کاربران در پذیرش نوآوری کافی نیست. آنها پیشنهاد کرده‌اند که باید سازه‌ها شامل حریم خصوصی، امنیت و درک خطر ایمنی و خودکارآمدی باشد (جهانگیر و بیگام، ۲۰۰۸)

برخی از محققان پیشنهاد کردند که اطلاعات جمعیتی مصرف‌کنندگان مانند تحصیلات، جنس، سن و غیره با سازه‌های TAM در نظر گرفته شود تا قصد رفتاری کاربران برای توضیح تصویب نوآوری توضیح داده شود (پرامپ آتانا پاکدی، ۲۰۰۹). همچنین مدل IDT (راجرز، ۱۹۶۲) برای توضیح کاربران برای اتخاذ یک فن‌آوری جدید/سیستم جدید مناسب‌تر است (راجرز، ۱۹۶۲) برخی از محققان TAM & IDT را در توضیح تصویب سیستم اطلاعات در رشته‌های مختلف ادامه داده‌اند (چن و همکاران، ۲۰۰۲؛ آه و همکاران، ۲۰۰۳؛ کیم و شین، ۲۰۱۵).

1. Internet of Things

2. Interoperable

مبانی نظری تحقیق

حریم خصوصی: پذیرش حریم خصوصی به عنوان یک حق انسانی ریشه‌ای تاریخی دارد. در قرآن، انجیل، یهود و چین باستان مصونیت‌هایی در این زمینه وجود داشته است (بروجردی ۲۰۰۴) برخی نویسندگان سابقه این حق را به دوران رم و یونان باستان نسبت می‌دهند و منشا آن را همان لزوم رعایت حق مالکیت نسبت به اموال مادی می‌دانند (محسنی ۲۰۰۱). خط و مشی حریم خصوصی در یک ارائه دهنده خدمات اینترنت، رعایت مسائل مرتبط با استفاده از اطلاعات شخصی کاربران می‌باشد (کوستا و دامورتییر ۲۰۰۸)

امنیت در اینترنت اشیاء: اینترنت اشیاء بخش جدایی‌ناپذیر از آینده اینترنت است. پروتکل‌های ارتباطی جدید هم به عنوان بنیاد این شبکه پیچ در پیچ ایفای نقش می‌کنند. وظیفه این پروتکل‌ها این است که تعامل و یکپارچگی کامل اشیاء مجازی و فیزیکی جهان پیرامون مان را تضمین کنند. کامپیوترها، گوشی‌ها، تلویزیون‌ها، حسگرها، خودروها و... در این شبکه متشکل از اشیاء قرار می‌گیرند.

لیکن خطراتی در اینترنت اشیاء وجود دارد و به همین دلیل نمی‌توان امنیت آن را صد در صد دانست. در اینترنت اشیاء دستگاه‌ها اطلاعاتی را فرستاده و دستوراتی را دریافت می‌کنند، از این رو نفوذ هکر و سوء استفاده آن چندان هم دور از انتظار نیست.

پیشینه پژوهش

در راستای هدف تحقیق به مطالعه بررسی‌های انجام‌شده در حوزه امنیت صنعت بانکداری و پذیرش آن در دیدگاه محققین مختلف پرداخته می‌شود.

در زمینه شرکت‌های مبتنی بر خدمات، صنعت بانکداری تجاری یکی از بخش‌هایی است که پذیرش نوآوری در فن آوری، منجر به تغییرات قابل توجهی در فرآیندهای عملیاتی شده است (علم، ۲۰۰۳).

صنعت بانکداری با یک رقابت سریع در حال تغییر، روبرو است. منظره‌ای که بر ارتباط و سودآوری آینده بانک‌های سنتی فشار می‌آورد. عدم اطمینان اقتصادی، رقابت شدید و مشتریانی که خواسته‌های بیشتری دارند مجموعه‌ای بی‌سابقه از چالش‌ها را ایجاد کرده است. بانک‌ها چندین سال است که در خدمات پیچیده و پیشرو سرمایه‌گذاری می‌کنند تا احساس عملکرد مدرن و دیجیتالی را ایجاد کنند. مبحث مدیریت نوآوری در بانک‌ها، علاقه جامعه علمی را برانگیخته است.

تیپو (۲۰۱۱) ۲۵۵ مقاله ژورنالی را در مورد مدیریت نوآوری در بانک‌ها مورد تجزیه و تحلیل قرار داد و نشان داد که اگرچه طیف گسترده‌ای از مقالات در این زمینه منتشر شده است، اما تعداد کمی از آنها به مدل‌ها و استراتژی‌های پذیرش نوآوری در صنعت بانک اختصاص یافته است. برخی از آنها بر روی عوامل موفقیت آمیز نوآوری در بانک‌ها متمرکز بودند که عوامل رضایت کاربر، سادگی، سرعت نوآوری، تمایز، تناسب محصول در درون سازمان و بازاریابی داخلی را شناسایی می‌کند؛ (گوپالاکریشنان و دامنیپور، ۲۰۰۰).

توجه ما برای نوآوری در روند مدیریت امنیت بانک‌ها مربوط به فرصت‌های بهبود عملکرد از طریق نوآوری خاص اینترنت اشیاء است.

هافمن و همکاران (۲۰۱۵) ادغام BPM در زمینه‌های خطر و امنیت را ترویج می‌کند زیرا ریسک و امنیت اهداف کارآیی و اثربخشی و سایر مولفه‌های ساختاری مانند فرایندهای ناشی از وقایع و زمان را با تکیه بر پشتیبانی انسان به اشتراک می‌گذارند. استفاده از روش BPR در مدیریت امنیت بانک‌ها باید به ویژگی‌های خاص دامنه مانند فرآیندهای غیرروتین/منحصر به فرد، فشار زمانی/فوریت، دخالت چندین مقام و بازیگر، و همچنین عدم وجود اطلاعات دقیق توجه کند. (سوئسون و پالمر، ۲۰۱۰) ماهیت کاملاً محرمانه اطلاعات، دسترسی به منابع مستقیم داده‌های ثانویه را محدود می‌کند.

صنعت بانکداری با یک فضای رقابتی به سرعت در حال تغییر مواجه است که فشار بر ارتباط و سودآوری آینده بانک‌های سنتی را تحت فشار قرار می‌دهد. از آنجا که عدم اطمینان اقتصادی، رقابت شدید و مشتریانی که بیشتر طلب می‌کنند،

مجموعه‌ای از چالش‌های بی‌سابقه را ایجاد کرده‌اند، بانک‌ها برای چندین سال در خدمات پیش‌رو سرمایه‌گذاری کرده‌اند تا تصور یک عملیات دیجیتال مدرن را ایجاد کنند. (سالوادور آمبریتو و همکاران ۲۰۱۸)

امنیت "به معنای یک محیط پایدار و نسبتاً قابل پیش‌بینی است که در آن یک فرد یا گروه ممکن است اهداف خود را بدون ایجاد اختلال و صدمه و بدون ترس از چنین مزاحمت یا صدمه‌ای دنبال کند" (فیشر و گرین، ۲۰۰۴، ص ۲۱).

برای بهبود درجه امنیت کلی بانک‌ها، گروه‌های بانکی از یک سیستم محافظتی استفاده می‌کنند که برای تعریف چگونگی مدیریت اقدامات حفاظتی برای کاهش ریسک عملیاتی، بنابراین بهبود درجه امنیت، با محافظت از دارایی‌های فیزیکی و غیر فیزیکی اساسی است. متأسفانه، اقدامات حفاظتی هنوز به اندازه کافی موثر نیستند و سیستم‌های حفاظتی کلی از استانداردهای امنیتی جهانی برخوردار نیستند (ای بی اف، ۲۰۱۶).

وقتی با بودجه کلی که موسسات بانکی برای شبکه‌های بانکی خود تصویب می‌کنند مقایسه می‌شود، هزینه راه‌اندازی و مدیریت یک سیستم حفاظت بسیار زیاد است در حالی که کارایی عملیاتی آن پایین است (اف بی ای، ۲۰۱۶). این مشکل در بخش بانکها به خوبی شناخته شده است و همچنان از بانکها خواسته می‌شود تا سیستمهای حفاظتی خود را به روز کنند، آنها را به روز نگه دارند و سیستم‌های پیشگیری را به طور مثر برای مقابله با حملات احتمالی جنایی اجرا کنند (ترندمیکرو، ۲۰۱۴).

یک روش برای حمایت از تصمیم اتخاذ اینترنت اشیا

امنیت "به معنای یک محیط پایدار و نسبتاً قابل پیش‌بینی است که در آن یک فرد یا گروه ممکن است اهداف خود را بدون ایجاد اختلال و صدمه و بدون ترس از چنین مزاحمت یا صدمه‌ای دنبال کند" (فیشر و گرین، ۲۰۰۴، ص ۲۱). برای بهبود درجه امنیت کلی بانک‌ها، گروه‌های بانکی از یک سیستم محافظتی استفاده می‌کنند که برای تعیین چگونگی مدیریت اقدامات حفاظتی برای کاهش ریسک عملیاتی و در نتیجه ارتقاء درجه امنیت، با محافظت از دارایی‌های فیزیکی و غیر فیزیکی، اساسی است. متأسفانه، اقدامات حفاظتی هنوز به اندازه کافی موثر نیستند و سیستم‌های حفاظتی کلی از استانداردهای امنیتی جهانی برخوردار نیستند (اف بی ای، ۲۰۱۶). هنگامی که با بودجه کلی موسسات بانکی برای شبکه‌های بانکی خود مستقر می‌شوند مقایسه می‌شود، هزینه راه‌اندازی و مدیریت یک سیستم محافظتی بالا است در حالی که بهره‌وری عملیاتی آن پایین است (اف بی ای، ۲۰۱۶) این مشکل در بخش بانک‌ها به خوبی شناخته شده است و همچنان از بانکها خواسته می‌شود تا سیستم‌های حفاظتی خود را به روز کنند، آنها را به روز نگه دارند و سیستم‌های پیشگیری را به طور موثر برای مقابله با حملات احتمالی جنایی اجرا کنند (ترندمیکرو، ۲۰۱۴).

با توجه به شدت مشکلات شناسایی شده در ادبیات دانشگاهی ناشی از خطر، فرایندهای امنیتی و خواسته‌های جدید اینترنت اشیا برای بهینه‌سازی عملیات بانکی، ما عناصر اصلی مورد نیاز برای مهندسی مجدد فرایند مدیریت امنیت بانک‌ها را در یک سیستم حفاظت هوشمند (IPS) شناسایی کردیم. هافمن و همکاران (۲۰۱۵) ادغام BPM در زمینه‌های خطر و امنیت را تقویت می‌کند زیرا خطر و امنیت اهداف بهره‌وری و اثربخشی و سایر مولفه‌های ساختاری مانند فرآیندهای مبتنی بر رویداد و زمان را با تکیه بر پشتیبانی انسان به اشتراک می‌گذارند.

منابع مستقیم داده‌های ثانویه. بیشتر ادبیات علمی قابل دسترس محققان شامل آماری در مورد حملات علیه بانک‌ها و اقدامات حفاظتی یا پروفایل جرم‌شناسی است. یافتن منابع مستقیم داده‌های ثانویه دشوار است مانند گزارش‌های رسمی یا اوراق سفید تولید شده توسط موسسات بانکی.

فرضیه‌ها و مدل مفهومی

کسب دانش در مورد یک فناوری جدید به کاربر کمک می‌کند تا به راحتی آن فناوری را به کار گیرد و از آن استفاده کند (لو و همکاران، ۲۰۰۳). دانش استفاده از رایانه و اینترنت ثابت کرده است که توانمندی خوبی برای پذیرش توسط کاربران دارد زیرا آنها را در استفاده از یک فناوری جدید از طریق سودمندی درک شده تحت تأثیر قرار می‌گیرند. (گارتینگ و اندابیسی، ۲۰۰۶)، علاوه بر این، مشاهده می‌شود که سازگاری به این واقعیت بستگی دارد که دانش کاربران تا چه حد از پذیرش فناوری

جدید پشتیبانی می‌کند و شخصی که احساس منفی نسبت به فناوری جدید دارد و به سختی ممکن است که از آن فناوری جدید استفاده کند را در این راستا متقاعد می‌کند. (رامایا و همکاران ۲۰۰۳). علاوه بر این، افرادی که در زمینه استفاده از رایانه و اینترنت دانش و تجربه دارند، احساس می‌کنند که استفاده از فناوری جدید مبتنی بر اینترنت، به دلیل رعایت حریم خصوصی و امنیت، خطر کمتری خواهد داشت. کنترل و دانش کمتر نسبت به مکانیسم مربوط به وب در کاربران باعث می‌شوند تا آن‌ها نسبت به حریم خصوصی و مسائل امنیتی حساس شوند (مک لنیس، ۲۰۰۵). با تمام این اطلاعات، فرضیه‌های زیر توسعه می‌یابد:

در این مقاله فرضیه‌های اصلی مدل TAM در پذیرش فناوری اینترنت به شرح ذیل معرفی شده است:

‡امنیت

‡مفید بودن؛

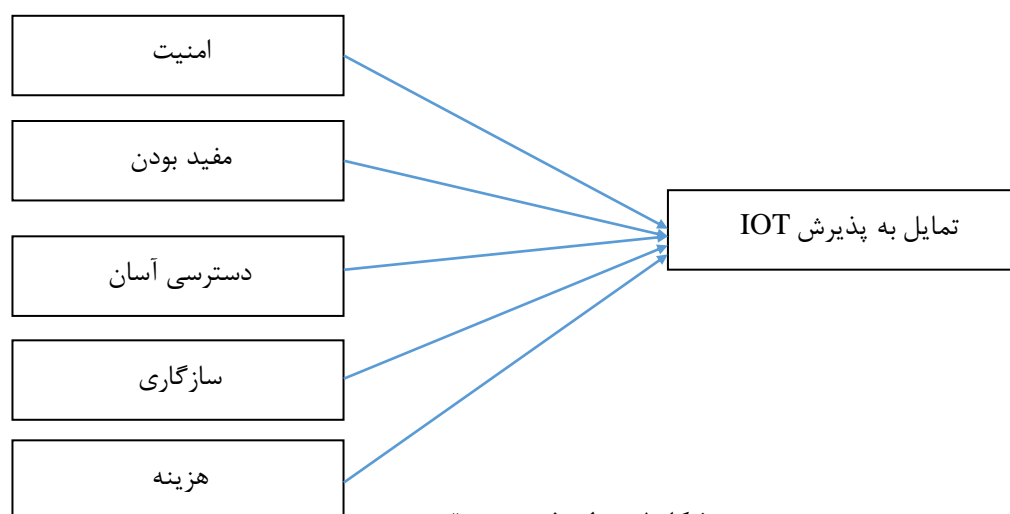
‡دسترسی آسان؛

‡سازگاری؛

‡هزینه؛ (شاترجی و خراق پور، ۲۰۲۰).

مدل مفهومی

مدل مفهومی نشان‌دهنده فناوری‌های موردنظر در یک پژوهش و رابطه بین آن‌هاست. در پژوهش حاضر از مدل TAM استفاده شده است. شکل (۱) مدل مفهومی مورداستفاده در این پژوهش را نشان می‌دهد.



شکل ۱: مدل مفهومی تحقیق

بدین ترتیب فرضیه‌های تحقیق حاضر به صورت ۵ فرضیه به شرح زیر تنظیم می‌گردد:

- فرضیه اول: خطرات حریم خصوصی و امنیت بر تمایل کاربران شعب بانک کشاورزی بر پذیرش اینترنت اشیا تاثیر دارد.
- فرضیه دوم: مفید بودن و سودمندی ادراک شده بر تمایل کاربران شعب بانک کشاورزی بر پذیرش اینترنت اشیا تاثیر دارد.
- فرضیه سوم: دسترسی آسان بر تمایل کاربران شعب بانک کشاورزی بر پذیرش اینترنت اشیا تاثیر دارد.
- فرضیه چهارم: سازگاری ادراک شده بر تمایل کاربران شعب بانک کشاورزی بر پذیرش اینترنت اشیا تاثیر دارد.
- فرضیه پنجم: هزینه بر تمایل کاربران شعب بانک کشاورزی بر پذیرش اینترنت اشیا تاثیر دارد.

روش تحقیق

برای جمع آوری داده ها، پرسشنامه ای تهیه شده است. موارد یا پرسشنامه از دانش متغیرها، از دانش حاصل از بررسی ادبیات و از دانش به دست آمده از TAM و IDT تهیه شده است. با این حال، موارد مربوط به حریم خصوصی و خطر امنیتی و هزینه و سازگاری آنها از مطالعات برخی از کارهای تحقیقاتی اقتباس شده است (مور و بن باسات، ۱۹۹۱؛ کیم و شین، ۲۰۱۵). از آنجا که اینترنت اشیا یک فناوری جدیدی است که پیرامون آن پرسشنامه تهیه شده است، تصور می شد که ممکن است مشکلاتی در به دست آوردن یک نمونه جامع و به همین ترتیب نمونه گیری راحت به عنوان یک روش همجنس برای جمع آوری داده های تحقیق وجود داشته باشد. پرسشنامه از طریق حضور در شعب بانک کشاورزی به کاربران داده شد و طی یک دوره ۱۹ روزه در تیر ماه ۱۴۰۰، ۵۶ پاسخ دریافت شده است. از میان ۵۶ پاسخ، یک پاسخ مبهم بود زیرا بعضی از پاسخ ها خالی بود و علامت تیک را در هیچ گزینه ای قرار نداشت این ۱ پاسخ مبهم در نظر گرفته و از ارزیابی ها حذف شد. اندازه نمونه (۵۵) قابل قبول به نظر می رسد. از این رو، کار نظرسنجی با ۲۳ ماده و ۵۵ پاسخ آغاز شد که در مقیاس ۵ درجه ای لیکرت تعیین شد.

یافته های تحقیق

جزئیات نظرسنجی

جزئیات جمعیتی در جدول ۱ نشان داده شده است. به نظر می رسد از ۵۵ پاسخ دهنده قابل استفاده، ۴۱ پاسخ مرد (۷۵/۹ درصد) و ۱۴ نفر زن (۲۴/۱ درصد) پاسخ داده اند. به نظر می رسد که حداکثر نمایندگی از محدوده سنی ۴۰-۳۰ سال وجود دارد. ۲۳ از ۵۵ (۴۱/۴٪) بود. تا آنجا که به مدارک تحصیلی مربوط می شود، حداکثر پاسخ دهندگان دارای مدرک کارشناسی ارشد ۲۳ از ۵۵ (۴۱/۴٪) است. برای اندازه گیری روایی و پایایی بررسی قابلیت اطمینان متغیرها، مقادیر آلفای کرونباخ برای هر متغیر درون زا محاسبه شده است. که نتایج آلفای کرونباخ در جدول ۲ نشان داده شده است. نتایج نشان می دهد که مقدار هر آلفای کرونباخ برای هر متغیر بیشتر از ۰/۶ است که حداقل مقدار قابل قبول است. از این رو متغیرهای درون زا به شماره ۷ قابل اعتماد هستند. سوال از قابلیت اطمینان دو متغیر دیگر (جنسیت و سن) بی اهمیت است.

شاخص پایایی

اکنون ضروری است که مشخص شود آیا هر متغیر می تواند ساختار خود را به درستی توضیح دهد یا خیر. برای اطمینان از این موضوع، فاکتور بارگذاری هر متغیر با توجه به ساختار خود تخمین زده می شود. نتایج در جدول ۳ نشان داده شده است.

جدول ۱. جزئیات جمعیتی پاسخ دهندگان

گروه ها		تعداد	درصد
جنسیت	مرد	۴۱	٪۷۵/۹
	زن	۱۴	٪۲۴/۱
سن	سال <۲۰	۰	٪۰
	سال ۲۱-۳۰	۱۲	٪۲۱
	سال ۳۱-۴۰	۲۳	٪۴۱/۴
	سال ۴۱-۵۰	۱۴	٪۲۶/۳
	سال > ۵۰	۶	٪۱۰/۵۲
تحصیلات	دیپلم	۰	٪۰
	فوق دیپلم	۶	٪۱۰/۵۲

لیسانس	۲۰	٪۳۶/۸۴
فوق لیسانس	۲۳	٪۴۱/۴
دکتری	۶	٪۱۰/۵۲

جدول ۲. نتایج آلفای کرونباخ برای روایی متغیرها

متغیرها	نتایج آلفای کرونباخ
(UK) دانش کاربران	0.896
(PU) مفید بودن	0.910
(PEOU) دسترسی آسان	0.887
(COM) سازگاری	0.879
(SPR) حریم خصوصی و امنیت	0.910
(COS) هزینه	0.922
(BI) تمایل کاربران	0.899

کمترین مقدار قابل قبول ضریب بارگذاری ۰/۷۰۷ است (گوتز و همکاران، ۲۰۱۰). از جدول بالا به نظر می‌رسد که از ۲۳ مورد نشان داده شده در جدول ۳، مقدار فاکتورهای بارگیری در ۳ مورد کمتر از ۰/۷۰۷ هستند و از این رو برای اعتبار آزمون در نظر گرفته نشده‌اند. بنابراین، از این پس با ۲۰ مورد برخورد خواهیم کرد.

قابلیت اطمینان متغیرها و روایی همگرا برای اطمینان از اعتبار متغیرها

برای اطمینان از اعتبار متغیرها، قابلیت اطمینان کامپوزیت (CR) برآورد شده است. همچنین، تأیید اعتبار همگرا ضروری است (فورنر و لارکر، ۱۹۸۱) که برای دستیابی به این هدف، میانگین واریانس استخراج شده (AVE) برآورد شده است. نتایج بارهای قابل قبول همراه با برآورد CR و همچنین AVE در جدول زیر نشان داده شده است.

جدول ۳. برآورد عوامل بارگیری

متغیرها / آیتم‌ها	فاکتور بارگزاری شده
دانش کاربران (UKN)	
UKN 1	0.96
UKN 2	0.89
UKN 3	0.46
UKN 4	0.92
سودمندی ادراک شده (PU)	
PU 1	0.95
PU 2	0.94
PU 3	0.91
دسترسی آسان ادراک شده (PEOU)	
۱ PEOU	0.98
۲ PEOU	0.96
3 PEOU	0.95
۴ PEOU	0.89
سازگاری (COM)	
۱ COM	0.92
۲COM	0.90

۳COM	0.88
خطر امنیت و حریم خصوصی (SPR)	
۱ SPR	0.96
۲ SPR	0.94
۳ SPR	0.47
هزینه (COS)	
۱ COS	0.89
۲ COS	0.98
۳ COS	0.49
تمایل کاربران (BI)	
BI 1	0.98
BI 2	0.96
BI 3	0.94

اگرچه فاکتورهای بارگیری در رابطه با SPR ۳ (۰.۴۷) و UKN ۳ (۰.۴۶) و COS ۳ (۰.۴۹) در جدول فوق نشان داده شده است، اما آنها در برآورد AVE و CR مربوطه در نظر گرفته نشده اند زیرا مقادیر آنها کمتر از پایین ترین حد قابل قبول است مقدار فاکتور بارگیری که ۰/۷۰۷ است. (گوتز ۲۰۱۰)

از جدول ۴ به نظر می رسد که تمام مقادیر CR از ۰.۶ بیشتر است که کمترین مقدار قابل قبول (اوربیچ و آهلیمان ۲۰۱۰). اعتبار متغیر را تأیید می کند. همچنین از این جدول به نظر می رسد که مقدار AVE هر متغیر درون زا بیشتر از حد قابل قبول است.

جدول ۴. برآورد بارهای قابل قبول همراه با CR و AVE

متغیرها / آیتم ها	فاکتور بارگزاری شده	CR	AVE
دانش کارران (UKN)		0.871	0.853
UKN 1	0.96		
UKN 2	0.89		
UKN 3	0.46		
UKN 4	0.92		
سودمندی ادراک شده (PU)		0.904	0.871
PU 1	0.95		
PU 2	0.94		
PU 3	0.91		
دسترسی آسان ادراک شده (PEOU)		0.921	0.894
۱ PEOU	0.98		
۲ PEOU	0.96		
3 PEOU	0.95		
۴ PEOU	0.89		
سازگاری (COM)		0.853	0.810
۱ COM	0.92		
۲COM	0.90		
۳COM	0.88		
خطر امنیت و حریم خصوصی (SPR)		0.936	0.903
۱ SPR	0.96		

۲ SPR	0.94		
۳ SPR	0.47		
هزینه (COS)		0.901	0.876
۱ COS	0.89		
۲ COS	0.98		
۳ COS	0.49		
تمایل کاربران (BI)		0.963	0.922
BI 1	0.98		
BI 2	0.96		
BI 3	0.94		

کمترین مقدار ۰.۵ (گیفتن و استروب، ۲۰۰۵؛ هیر، ۲۰۰۶) که تایید می کند اعتبار همگرا ایجاد شده است. آزمون اعتبار متمایز هنگامی که مشاهده می شود موارد مربوط به هر متغیر به شدت با آن متغیر مرتبط هستند و با متغیرهای دیگر ضعیف هستند، این اعتبار را تایید می کند. اگر فاکتورهای بارگیری از عوامل بارگذاری متقابل بیشتر باشد، اعتبار تفکیکی را تایید می کند. علاوه بر این، روش دیگری نیز برای تایید این موضوع وجود دارد. اگر مشخص شود که ریشه مربع هر AVE مربوط به یک متغیر بیشتر از ضرایب همبستگی آن متغیر با متغیرهای دیگر است، تایید می شود که اعتبار متمایز تاسیس شده است. (فورنل و لارکر ۱۹۸۱، گیفن و استروب ۲۰۰۵). این نتایج در جدول ۵ و در جدول ۶ نشان داده شده است.

جدول ۵. عوامل بارگیری و بارگیری متقابل

مقیاس	دانش	جنسیت	سن	مفید بودن	دسترسی آسان	سازگاری	امنیت	هزینه	تمایل کاربران
UKN 1	0.96	0.66	0.52	0.11	0.65	0.66	0.55	0.66	0.52
UKN 2	0.89	0.52	0.57	0.65	0.62	0.67	0.54	0.65	0.56
۴UKN	0.92	0.49	0.51	0.42	0.69	0.68	0.62	0.67	0.57
GENDER	0.66	1.00	0.62	0.54	0.52	0.56	0.62	0.62	0.58
AGE	0.58	0.62	1.00	0.61	0.62	0.60	0.67	0.55	0.62
PU 1	0.62	0.61	0.61	0.95	0.41	0.41	0.47	0.53	0.67
PU 2	0.52	0.58	0.57	0.94	0.39	0.45	0.41	0.47	0.47
PU 3	0.43	0.62	0.49	0.91	0.46	0.55	0.52	0.48	0.48
۱ PEOU	0.49	0.67	0.44	0.62	0.98	0.59	0.57	0.62	0.61
۲ PEOU	0.47	0.49	0.42	0.63	0.96	0.62	0.51	0.66	0.51
PEOU3	0.51	0.58	0.66	0.56	0.95	0.61	0.62	0.46	0.41
۴ PEOU	0.62	0.66	0.62	0.44	0.89	0.48	0.47	0.41	0.47
۱ COM	0.61	0.52	0.41	0.48	0.47	0.92	0.62	0.38	0.31
۲ COM	0.59	0.49	0.49	0.49	0.62	0.90	0.67	0.44	0.44
۳ COM	0.53	0.44	0.49	0.41	0.69	0.88	0.69	0.39	0.32
۱ SPR	0.46	0.61	0.62	0.62	0.48	0.47	0.96	0.21	0.57
۲ SPR	0.60	0.43	0.63	0.59	0.44	0.49	0.94	0.62	0.61
۱ COS	0.56	0.44	0.48	0.44	0.49	0.51	0.62	0.89	0.44
۲ COS	0.52	0.56	0.49	0.51	0.46	0.62	0.61	0.98	0.62
BI 1	0.61	0.62	0.56	0.55	0.58	0.66	0.69	0.67	0.98
BI 2	0.66	0.61	0.52	0.59	0.62	0.67	0.51	0.69	0.96
BI 3	0.63	0.67	0.51	0.60	0.61	0.49	0.49	0.62	0.94

به نظر می‌رسد بارگیری موارد مربوط به سازه خود مقادیر بالاتری نسبت به بارگذاری موارد مربوط به سایر متغیرها داشته باشد که اعتبار تمایز را تأیید می‌کند. از جدول فوق به نظر می‌رسد که عناصر مورب ریشه‌های مربعی AVE (معروف به AV) هستند که همگی از ضرایب تصحیح خارج مورب بیشتر هستند. همچنین اعتبار متمایز را تعیین می‌کند. جدول ۵ و جدول ۶ هر دو اعتبار تبعیض را تأیید می‌کنند.

مدل ساختاری

این فرایندی است که به کمک آن می‌توان مدل مناسب ارائه شده را آزمایش کرد یا خیر. برای انجام این کار، باید شاخص‌های متناسب را پیدا کنیم. در اینجا ما از تکنیک مدل‌سازی معادلات ساختاری کمک گرفته ایم، بستگی به تجزیه و تحلیل حداقل مربعات جزئی (PLS) دارد (گیفن و همکاران، ۲۰۰۰). نتایج در جدول ۷ نشان داده شده است.

جدول ۶. ارزیابی اعتبار متمایز

	UKN	PU	PEOU	COM	SPR	COS	BI	AVE
UKN	0.924							0.853
PU	0.591	0.933						0.871
PEOU	0.609	0.584	0.945					0.894
COM	0.701	0.608	0.611	0.900				0.810
SPR	0.919	0.599	0.705	0.627	0.950			0.903
COS	0.691	0.617	0.639	0.567	0.711	0.936		0.876
BI	0.662	0.693	0.661	0.696	0.590	0.621	0.960	0.922

جدول ۷. شاخص‌های مناسب مدل‌سازی معادلات ساختاری

شاخص‌های متناسب	استاندارد	تخمین زده شده	ملاحظات
$\frac{2}{df}$	$1 < \frac{2}{df} < 3$ (کلین، ۲۰۰۵)	1.876	به نظر می‌رسد که مقدار ۱.۸۷۶ است که درون آن است محدوده مجاز و از این رو قابل قبول است.
شاخص تطبیقی مقایسه‌ای (CFI)	> 0.93 (هیر و همکاران، ۲۰۰۶)	0.972	به نظر می‌رسد که مقدار CFI ۰.۹۷۲ است که می‌باشد و بیش از ۰.۹۳ بنابراین قابل قبول است.
(NFI) شاخص مناسب عادی	> 0.95 (شوماکر و همکاران، ۲۰۰۴)	0.976	مقدار NFI ۰.۹۷۶ است که بیشتر از ۰.۹۵ است و بنابراین قابل قبول است.
(TLI) شاخص تاکر لوئیس	> 0.91 (شارما و همکاران، ۲۰۰۵)	0.962	مقدار TLI ۰.۹۶۲ است که بیشتر از ۰.۹۱ است و بنابراین قابل قبول است.
خطای میانگین مربع ریشه (RMSE)	< 0.08 (اشتایگر، ۲۰۰۷)	0.009	مقدار RMSE ۰.۰۰۹ است که نزدیک به ۰ است و بدیهی است کمتر از ۰.۰۸ است و بنابراین قابل قبول است.

نتایج نشان می‌دهد که تمام شاخص‌های تناسب در محدوده قابل قبولی هستند که تأیید کننده پذیرفتن مدل هستند (موریسون و همکاران، ۲۰۱۷). با تمام این بحث‌ها، ما مدل متوسط اثر را در شکل ۲ نشان داده ایم.

بحث درباره نتایج

از آزمایش فرضیه‌ها با استفاده از PLS به نظر می‌رسد که سودمندی (PU) می‌تواند تا $R^2 = 0.69$ (۶۹٪) توسط دانش کاربران (UKN)، جنسیت (GEN)، سن و سهولت استفاده (PEOU) توضیح داد.

سهولت استفاده (PEOU) را می‌توان با دانش کاربران (UKN)، جنسیت (GEN)، سن (AGE) و سازگاری تا ۶۱٪ (R2=0.61) توضیح داد.

(COM) باز هم دانش کاربران (UKN)، جنسیت (GEN) و سن (AGE) می‌تواند خطر امنیت و حریم خصوصی (SPR) را تا ۵۷٪ (R2=0.57) توضیح دهند و تأثیر سازگاری (COM) ($\beta = -0.012$) بر فرضیه رد امنیت و امنیت حریم خصوصی SPR ۱۰٪ ناچیز است

دوباره سازگاری (COM) را با دانش کاربران (UKN)، جنسیت (GEN) و سن (AGE) می‌توان تا ۵۲٪ توضیح داد. بسیار جالب است که این سه متغیر اصلی (UKN، GEN و AGE) تقریباً به طور مساوی بر سازگاری (COM) تأثیر مثبت می‌گذارند زیرا ضرایب مسیر برای این سه مورد بسیار نزدیک هستند یعنی ($\beta = 0.322$) $UKN \rightarrow COM$ و ($\beta = 0.344$) $AGE \rightarrow COM$.

جنسیت (GEN) و سن (AGE) می‌توانند هزینه (COS) را تا حدود ۴۳٪ توضیح دهند (R2=0.43). تمایل کاربران بانک را می‌توان با استفاده از درک مفید بودن (PU)، سهولت استفاده (PEOU)، سازگاری (COM)، خطر امنیت و حریم شخصی (SPR) و هزینه (به میزان ۸۲٪ (R2=0.82) توضیح داد. که به نظر می‌رسد حداکثر سهم مثبت بر تمایل کاربران از سازگاری ناشی می‌شود زیرا ضریب مسیر مربوط به آن مرتفع‌ترین است ($\beta = 0.748$). خطر امنیت و حریم خصوصی (SPR) بر تمایل کاربران تأثیر منفی می‌گذارد. ($\beta = -0.679$). هزینه (COS) هم بر تمایل کاربران نیز تأثیر منفی می‌گذارد ($\beta = -0.528$). خطر امنیت و حریم خصوصی (SPR) بیشتر بر تمایل کاربران در مقایسه با هزینه (COS) تأثیر منفی می‌گذارد، زیرا به نظر می‌رسد مقدار منفی β در مورد SPR-BI بیشتر باشد.

سازگاری (COM) و سهولت استفاده (PEOU) هر دو به ترتیب از طریق PEOU و از طریق PU به طور غیر مستقیم بر تمایل کاربران تأثیر می‌گذارند. در زمینه اثرات مثبت، اثر سازگاری (COM) بر تمایل کاربران است. و سودمندی (PU) بیشترین تأثیر مثبت ($\beta = 0.672$) را بر تمایل کاربران بانکی دارد. کل سناریو به طور خلاصه در جدول ۸ نشان داده شده است. به طور خلاصه، نتایج برجسته:

- دانش کاربر (UKN) بر PEOU، COM و SPR تأثیر مثبت می‌گذارد.
- جنسیت (GEN) بر PU، PEOU، COM، SPR، COS تأثیر مثبت می‌گذارد.
- سن (AGE) بر PU، PEOU، COM تأثیر منفی می‌گذارد و (AGE) بر SPR و COS تأثیر مثبت می‌گذارد.
- PU، PEOU، COM تأثیر مثبتی بر کاربران دارد.
- SPR و COS تأثیر منفی بر کاربران دارند.
- COM و PEOU به ترتیب بر PEOU و PU تأثیر مثبت می‌گذارند.
- COM تأثیری در SPR ندارد و به همین دلیل این فرضیه پذیرفته نشده است (H10).

تأثیر تحقیقات

به نظر می‌رسد که سودمندی (PU)، سهولت استفاده (PEOU)، سازگاری (COM)، خطرات امنیتی و حریم خصوصی (SPR) و هزینه (COS) تأثیر مستقیم قابل توجهی بر تمایل کاربران بانکی برای استفاده از اینترنت اشیا دارد. همچنین به نظر می‌رسد که از بین این پنج باور مصرف کننده، سازگاری بیشترین تأثیر را بر تمایل رفتاری کاربران دارد که با برخی از کارهای تحقیقاتی قبلی مطابقت دارد. از این رو به نظر می‌رسد که اگر طراحی اینترنت اشیا با کاربران سازگار باشد، شانس موفقیت وجود دارد.

تأثيرات	فرضيه	جهت	ضريب مسير	تاييد مراحل	تاييد شده	ملاحظات
Effect on PU		R2 = 0.69				
By UKN	H1a	UKN→PU	0.498	P < 0.01	+	Accepted
By GEN	H2a	GEN→PU	0.621	P < 0.01	+	Accepted
By AGE	H3a	AGE→PU	0.216	P < 0.05	-	Accepted
By PEOU	H5	PEOU→PU	0.312	P < 0.01	+	Accepted
Effect on PEOU		R2 = 0.61				
By UKN	H1b	UKN→PEOU	0.263	P < 0.01	+	Accepted
By GEN	H2b	GEN→PEOU	0.411	P < 0.01	+	Accepted
By AGE	H3b	AGE→PEOU	0.414	P < 0.05	-	Accepted
By COM	H8	COM→PEOU	0.367	P < 0.01	+	Accepted
Effect on COM		R2 = 0.52				
By UKN	H1c	UKN→COM	0.322	P < 0.01	+	Accepted
By GEN	H2c	GEN→COM	0.322	P < 0.01	+	Accepted
By AGE	H3c	AGE→COM	0.344	P < 0.05	-	Accepted
Effect on SPR		R2 = 0.52				
By UKN	H1c	UKN→COM	0.322	P < 0.01	+	Accepted
By GEN	H2c	GEN→COM	0.322	P < 0.01	+	Accepted
By AGE	H3c	AGE→COM	0.344	P < 0.05	-	Accepted
Effect on SPR		R2 = 0.57				
By UKN	H1d	UKN→SPR	0.116	P < 0.01	+	Accepted
By GEN	H2d	GEN→SPR	0.216	P < 0.01	+	Accepted
By AGE	H3d	AGE→SPR	0.418	P < 0.01	+	Accepted
By COM	H10	COM→SPR	0.012	ns	-	Accepted
Effect of COS		R2 = 0.43				
By GEN	H2e	GEN→COS	0.214	P < 0.01	+	Accepted
By AGE	H3e	AGE→COS	0.226	P < 0.01	+	Accepted
Effect on BI		R2 = 0.82				
PU By	H6	PU→BI	0.672	P < 0.01	+	Accepted
By PEOU	H4	PEOU→BI	0.669	P < 0.01	+	Accepted
By COM	H7	COM→BI	0.748	P < 0.001		Accepted
By SPR	H9	SPR→BI	0.679	P < 0.05	-	Accepted
By COS	H11	COS→BI	0.528	P < 0.05	-	Accepted

خطرات امنیت و حریم خصوصی (SPR) تأثیر منفی قابل توجهی بر تمایل کاربران بانکی و استفاده کنندگان از اینترنت اشیا دارد. SPR مانع عمده ای برای پذیرش اینترنت اشیا توسط کاربران استفاده کننده خدمات بانک کشاورزی است. SPR ممکن است در آینده برای ایجاد انگیزه در کاربران بانک کشاورزی از اینترنت اشیا یک مشکل اساسی ایجاد کند (ای متریکس ۲۰۰۸). سپس نقش سودمندی (PU) ظاهر می شود که بر روی کاربران اینترنت اشیا تأثیر مثبت می گذارد. این با بسیاری از کارهای تحقیقاتی همخوانی دارد (اندویسی، ۲۰۰۷).

اگر کاربران بالقوه اینترنت اشیا را برای خود مفید بدانند، اینترنت اشیا را اتخاذ می کنند.

در مرحله نوآوری قبل از تصویب موضوع سهولت استفاده همانطور که در بسیاری از کارهای پژوهشی دیده می شود، نقشی حیاتی دارد (وانگ و همکاران، ۲۰۰۳)

کاربران بانک کشاورزی در مورد مسئله هزینه بسیار محتاط هستند. هزینه (COS) به طور قابل توجهی اما منفی بر تمایل کاربران تأثیر می گذارد.

مجدداً مشخص شد که سازگاری از طریق تاثیر سهولت استفاده PEOU تاثیر مستقیم و غیرمستقیم بر تمایل کاربران می گذارد که با کارهای تحقیقاتی قبلی مطابقت دارد (اوو و همکاران، ۲۰۰۳). همچنین مشاهده شده است که PEOU سهولت استفاده مطابق با سایر کارهای تحقیقاتی بر تمایل کاربران تأثیر مستقیم دارد (چان و لو، ۲۰۰۴).

تا آنجا که به تأثیر تفاوت‌های فردی مشتریان مربوط می شود، دانش کاربر (UKN) بر مطالعات تأیید آمیز PEOU، COM و SPR تأثیر مثبت می گذارد، در حالی که کاربران مرد با سن کمتر فکر می کنند که اینترنت اشیا تاکنون خطر کمتری دارد کاربران امنیت و حریم خصوصی نگران هستند. زنان و مصرف کنندگان پیر در مورد هزینه که سایر کارهای تحقیقاتی را نیز تأیید می کند بسیار آگاه هستند (رامایا و همکاران، ۲۰۰۳).

این مطالعه این واقعیت را روشن کرده است که اگر مدیران بانک کشاورزی به عنوان ارائه دهنده خدمات اینترنت اشیا بتوانند ویژگی های خدمات اینترنت اشیا را به طور مناسب مدیریت کنند، پذیرش اینترنت اشیا در این بانک افزایش می یابد. کاربران جوان خدمات بانکی کشور ممکن است به عنوان یک بازار مناسب در نظر گرفته شوند و می توان به آنها نفوذ کرد زیرا این جوانان می توانند بدون ترس از ویژگی های اینترنت اشیا از آن استفاده کنند. باید به کاربران و سیستم عامل های فن آوری پیشرفته و معطوف به این واقعیت توجه شود که استفاده کنندگان چه چیزهایی را مفید می دانند و چه چیز استفاده های آنها را آسان می کند. این امر باعث می شود کاربران اینترنت اشیا خدمات بانک کشاورزی را بیسندد و می توانند در یک محیط آموزنده مناسب فعالیت نمایند.

کاربران شعب بانک کشاورزی به طور کلی نسبت به خطر حفظ حریم خصوصی و امنیت بسیار محتاط هستند و از این رو ارائه دهندگان اینترنت اشیا بانک کشاورزی در ایران و در بخش های خصوصی و دولتی باید درک دقیق استفاده کنندگان در مورد خطر حریم خصوصی و امنیت را ارائه دهند.

بانک کشاورزی به عنوان ارائه دهنده خدمات اینترنت اشیا باید سیستم هایی را برای بهبود احراز هویت و مشکلات رمز عبور در پردازش توسعه دهد. آنها باید برای محافظت از داده های کاربران در برابر استفاده ثانویه غیر مجاز و تهیه خدمات جامع برای کاربران بالقوه ای که با مشکلات امنیت و حریم خصوصی روبرو هستند، برنامه جامعی ترتیب دهند.

برای افزایش آگاهی کاربران لازم است فعالیت های تبلیغاتی انجام شود. با راه اندازی برنامه آموزشی و آگاهی، باید به کاربران بانک کشاورزی این آگاهی را داد که چگونه فناوری اینترنت اشیا مفید است و می توان با آن راحت کار کرد.

محدودیت ها و دستورالعمل های پژوهشگران آینده

محدودیت اصلی این مطالعه مربوط به روند بررسی است. خوانش سوالات اگر با بیش از ۶ متخصص مشورت می کردیم شفاف تر بود.

برای هدف قرار دادن نمونه، ۶ حوزه سرپرستی مدیریت فناوری در کشور را انتخاب کردیم و در نهایت ۵۶ پاسخ دهنده قابل استفاده را انتخاب کردیم. ما باید بیش از ۶ حوزه مدیریتی فناوری اطلاعات و همچنین چندین بانک در شهر و سطح کشور و بیش از ۵۶ پاسخ دهنده قابل استفاده از جمله پاسخ دهندگان مناطق روستایی و کم برخوردار از فناوری را انتخاب کنیم. این می توانست نتیجه عمومی تری را ارائه دهد. همچنین ممکن است شرایط مرزی دیگری از جمله عادت، شرایط تسهیل کننده و غیره را مورد بررسی قرار دهیم تا بررسی کنیم چگونه می تواند مدل را بهبود بخشد. از آنجا که تصویب کامل اینترنت اشیا در بانک های کشور اتفاق نیفتاده است، ما با انجام نظرسنجی از کاربران بانک ها در خصوص اینترنت اشیا به نتیجه خوبی خواهیم رسید. و محققان آینده با در نظر گرفتن این محدودیت ها می توانند این نقاط کشف نشده را پرورش دهند.

نتیجه گیری

هدف اصلی این مطالعه تحقیقاتی شناسایی عواملی بود که می‌توانند بر تمایل کاربران برای استفاده از اینترنت اشیا از دیدگاه امنیت تأثیر مثبت یا منفی بگذارند. نتایج نشان داد که مدل ارائه شده به طور مفهومی پس از اعتبار سنجی مناسب می‌تواند عواملی را تعیین کند که تمایل کاربران را برای استفاده از اینترنت اشیا تعیین می‌کند. مدل ارائه شده، به بانک‌های با خدمات اینترنت اشیا کمک می‌کند تا به درستی استراتژی‌هایی برای توسعه خدمات جدید تدوین کنند، تا برنامه‌های تبلیغاتی را برای تسریع در پذیرش خدمات اینترنت اشیا در بین کاربران ارائه دهند. این مطالعه به عنوان منبع تعمق عمیق محققان برای بهبود قدرت تفکر آنها عمل کرد. دستگاه‌های فعال اینترنت اشیا با حجم عظیمی از داده‌ها از جمله داده‌های شخصی سروکار دارند. اینترنت اشیا یک فناوری مبتنی بر اینترنت است. از این رو، استفاده از دستگاه‌های مجهز به اینترنت اشیا باعث ایجاد امنیت و حریم خصوصی می‌شود (باروکاس و همکاران، ۲۰۱۴؛ حسین و همکاران، ۲۰۱۸). از این رو، ارائه دهندگان باید هوشیار و صادق باشند تا به کاربران آگاهی دهند که سیستم اینترنت اشیا به گونه‌ای توسعه یافته است که مکانیسم‌های داخلی برای محافظت از داده‌ها در برابر آسیب پذیری‌های امنیت و حریم خصوصی را تامین کند (هوتا و همکاران، ۲۰۱۵؛ زویدرون، ۲۰۱۴؛ اونیل و کاتی، ۲۰۱۷؛ سباستین و هارتمن، ۲۰۱۹). تا زمانی که به کاربران بالقوه اطلاع داده نشود که استفاده از اینترنت اشیا مخل حریم خصوصی و مسائل امنیتی آنها نیست، هیچ اعتمادی افزایش نخواهد یافت و کاربران بدون تردید از دستگاه‌های مجهز به اینترنت اشیا استفاده نمی‌کنند. به همین ترتیب، بانک کشاورزی درگیر انجام فعالیتهای تبلیغاتی برای آگاهی دادن مناسب کاربران نسبت به اقدامات محافظتی در دستگاه‌های اینترنت اشیا می‌باشد.

منابع و مراجع

- [۱] حبیبی، رویا، آل شیخ، علی اصغر، ارزیابی کیفیت سرویس های درون یابی مکانی در توسعه سامانه های پایش آلودگی هوا بر مبنای اشیاء نشریه علمی - پژوهشی علوم و فنون نقشه برداری، دوره ششم، شماره ۴، ۱۳۹۶.
- [۲] کارگر شریف آباد، محمد، گرامی، محسن، یزدان پناه، احمد علی، شناسایی فاکتورهای موثر در پذیرش اینترنتی اشیاء از دیدگاه کاربران با استفاده از مدل تکمیلی TAM ارائه شده در مدل گایو و بای. مورد مطالعه: مشتریان ارتباطات سیار ایران-همراه اول، فصلنامه رشد فناوری، سال پانزدهم، شماره ۵۸، ۱۳۹۸.
- [۳] جمالو، محمد، رجب زاده قطری، رادفر، رضا، طراحی مدلی به منظور امنیت اطلاعات و حفظ حریم خصوصی در اینترنت اشیاء، فصلنامه انتظام اجتماعی، سال دهم، شماره اول، ۱۳۹۷.
- [۴] قاسمی، روح اله، محقر، علی، صفری، حسین، اکبری جوکار، محمد رضا، اولویت بندی کاربردهای فناوری اینترنت اشیاء در بخش بهداشت و درمان ایران: محرکی برای توسعه پایدار، مدیریت فناوری اطلاعات، دانشکده مدیریت دانشگاه تهران، دوره ۸، شماره ۱، ۱۳۹۵.
- [۵] انصاری، منوچهر، محمدیان، ایوب، نویسنده، احسان، شناسایی کاربردهای اینترنت اشیاء در خلّه هوشمند با استفاده از روش فراترکیب، مدیریت فناوری اطلاعات، دانشکده مدیریت دانشگاه تهران، دوره ۹، شماره ۴، زمستان ۱۳۹۶.
- [6] Vahdat D. Internet of things. Tehran, Iran: Ati-Negar Publications; 2017. [In Persian].
- [7] K. Ayush, Suchetha, B., Sushila., S, Akshay, M., "Implementation of IoT (Internet of Things) and Image processing in smart agriculture," presented at the International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), 2016.
- [8] Farooq MU, Waseem M, Waseem M, Mazhar S, Khairi A. Talha Kamal. A Review on Internet of Things (IoT). International Journal of Computer Applications 2015; 113, 1: 1-7.
- [9] Acquity Group. (2014). *The Internet of Thing: the continuation of Internet*.
- [10] Agarwal, R., Rastogi, S., & Mehrotra, A. (2009). Customers' perspectives regarding e-banking in an emerging economy. *Journal of Retailing and Customer Services*, 16(5), 340–351. doi:10.1016/j.jretconser.2009.03.002
- [11] Algebhand, P. (2006). Adoption of electronic banking services by Iranian Customers [Master Thesis]. Lulea University of Technology, Lulea.
- [12] Bandyopadhyay, K., & Bandyopadhyay, S. (2010). User acceptance of Information Technology across cultures. *International Journal of Intercultural Information Management*, 2(3), 218–231. doi:10.1504/IJIM.2010.037862
- [13] Baner, K., & Hein, S. E. (2006). The effect of heterogeneous risk on the early adoption of internet banking technologies. *Journal of Banking & Finance*, 30(6), 1713–1725. doi:10.1016/j.jbankfin.2005.09.004
- [14] Barocas, S., & Nissenbaum, H. (2014). Big Data's End Run Around Procedural Privacy Protections. *Communications of the ACM*, 57(11), 31–33. doi:10.1145/2668897
- [15] Brown, E. (2016). *Who Needs the Internet of Things?* Linux. Retrieved from <https://www.linux.com/news/who-needs-internet-things>
- [16] Carpenter, S. (2018). Ten Steps in Scale Development and Reporting: A Guide for Researchers. *Communication Methods and Measures*, 12(1), 25–44. doi:10.1080/19312458.2017.1396583
- [17] Carstensen, L. L., Gottman, J. M., & Levenson, R. W. (1995). Emotional behavior in long-term marriage. *Psychology and Aging*, 10(1), 140–149. doi:10.1037/0882-7974.10.1.140 PMID:7779311
- [18] Celic, H. (2008). What determines Turkish customers' acceptance of internet banking? *International Journal of Bank Marketing*, 26(5), 353–370. doi:10.1108/02652320810894406
- [19] Chan, S. C., & Lu, M. T. (2004). Understanding internet banking adoption and use behavior: A Hong Kong perspective. *Journal of Global Information Management*, 12(3), 21–43. doi:10.4018/jgim.2004070102
- [20] Chatchawanwan, Y., Chaipoopiratana, S., & Combs, H. (2009). An investigation of the factors impacting customers' willingness of adopt internet banking in Thailand. In *Proceedings of ASBBS* (pp. 1-9). Academic Press.
- [21] Chen, L., Gillenson, M., & Sherrell, D. (2002). Enticing online consumers: An extended technology acceptance perspective. *Information & Management*, 39(8), 705–719. doi:10.1016/S0378-7206(01)00127-6

- [22] Cheng, T. C. E., Lam, D. Y. C., & Yeung, A. C. L. (2006). Adoption of internet banking: An empirical study in Hong Kong. *Decision Support Systems*, 42(3), 1558–1572. doi:10.1016/j.dss.2006.01.002
- [23] Choudhary, S., & Kesswani, N. (2019). A Survey: Intrusion Detection Techniques for Internet of Things. *International Journal of Information Security and Privacy*, 13(1), 86–105. doi:10.4018/IJISP.2019010107
- [24] Davis, F. D. (1989). Perceived usefulness and perceived ease of use and user acceptance of information technology. *Management Information Systems Quarterly*, 3(3), 319–340. doi:10.2307/249008
- [25] Deb, M., & David, E. L. (2014). An empirical examination of customers' adoption of m-banking in India. *Journal of Marketing Intelligence & Planning*, 32(4), 475–494. doi:10.1108/MIP-07-2013-0119
- [26] Deutsche Welle. (2012). *Internet of Things Holds Promise, but sparks Privacy concerns*. Retrieved from <http://www.dw.com/en/internet-of-things-holds-promise-but-sparks-privacy-concerns/a-15911207-1>
- [27] Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurements error. *JMR, Journal of Marketing Research*, 18(1), 39–50. doi:10.1177/002224378101800104
- [28] Gao, L., & Bai, X. (2014). A unified perspective on the factors influencing consumer acceptance of internet of things technology. *Asia Pacific Journal of Marketing and Logistics*, 26(2), 211–231. doi:10.1108/ technology acceptance model. *Management Information Systems Quarterly*, 21(4), 389–400. doi:10.2307/249720
- [29] Gefen, D., & Straub, D. (2005). A Practical Guide to Factorial Validity using PLS-Graph: Tutorial and Annotated Example. *Communications of the Association for Information Systems*, 16(2), 91–109.
- [30] Gefen, D., Straub, D., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems*, 4(7), 1–77.
- [31] Gotz, O., Lichr-Gobbers, K., & Krafft, M. (2010). Evaluation of Structural Equation Models using the Partial- Least-Square (PLS) Approach. In V. Esposito Vinzi, W.W. Chin., J. Henseler., and H. Wang (Eds), *Handbook of Partial Least Squares: Concepts, Methods and Applications* (pp. 691-711). Heidelberg: Springer.
- [32] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future direction. *Future Generation Computer Systems*, 29(7), 1645–1660. doi:10.1016/j.future.2013.01.010
- [33] Guriting, P., & Ndubisi, N. O. (2006). Borneo online banking evaluating customer perceptions and behavioral intention. *Management Research News*, 29(1-2), 6–15. doi:10.1108/01409170610645402
- [34] Hair, J., Anderson, R., Tatham, R., & Black, W. (1998). *Multivariate Data Analysis with Readings*. New York: McMillan.
- [35] Hair, J., Black, W., Babin, B., Anderson, R., & Tatham, R. (2006). *Multivariate Data Analysis* (6th ed.). New Jersey, USA: Pearson.
- [36] Haller, S., Karmouskos, S., & Schroth, C. (2009). The internet of things in an enterprise context. In J. Domingue, D. Fensel, and P. Traverso (Eds), *Future Internet* (pp. 14-28). Springer.
- [37] Harwood, T., & Garry, T. (2017). Internet of Things: Understanding trust in techno-service systems. *Journal of Service Management*, 28(3), 442–475. doi:10.1108/JOSM-11-2016-0299
- [38] Hirsch, P. B. (2019). The goose that laid the golden eggs: Personal data and the Internet of Things. *The Journal of Business Strategy*, 40(1), 48–52. doi:10.1108/JBS-10-2018-0176
- [39] Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind. Revised and Expanded* (3rd ed.). New York: McGraw-Hill.
- [40] Hota, C., Upadhyaya, S., & Al-Karaki, J. N. (2015). Advances in secure knowledge management in the big data era. *Information Systems Frontiers*, 17(5), 983–986. doi:10.1007/s10796-015-9593-y
- [41] Hussain, M., & Kaliya, N. (2018). An Improvised Framework for Privacy Preservation in IoT. *International Journal of Information Security and Privacy*, 12(2), 46–63. doi:10.4018/IJISP.2018040104

- [42] Jahangir, N., & Begum, N. (2008). The role of perceived usefulness, perceived ease of use, security and privacy and customer attitude to engender customer adaptation in the context of electronic banking. *African Journal of Business Management*, 2(1), 32–40.
- [43] Jayashankar, P., Nilakanta, S., Johnston, W. J., Gill, P., & Bures, R. (2018). IoT adoption in agriculture: The role of trust, perceived value and risk. *Journal of Business and Industrial Marketing*, 33(6), 804–821. doi:10.1108/JBIM-01-2018-0023
- [44] Kaur, R., Verma, K., Jain, S. K., & Kesswani, N. (2019). Efficient Routing Protocol for Location Privacy