مطالعه تجربی ادراکات مشتری از امنیت و اعتماد در سیستم های پرداخت الکترونیک

چکیده

یک باور عمومی این است که امنیت خوب موجب بهبود اعتماد شده و این که ادراک از امنیت و اعتماد خوب در نهایت موجب افزایش استفاده از تجارت الکترونیک می شود. در حقیقت، ادراک مشتریان از امنیت سیستم های پرداخت الکترونیکی به یک عامل عمده و اصلی در تکامل تجارت الکترونیک در بازار ها تبدیل شده است. در این مقاله، ما به بررسی مسائل مربوط به امنیت پرداخت الکترونیکی از دیدگاه مشتریان می پردازیم. این مطالعه یک مدل مفهومی را ارایه می کند که این مدل تعیین کننده عوامل موثر بر امنیت ادراک شده مصرف کننده ها و اعتماد ادراک شده آن ها و نیز اثرات امنیت ادراک شده و اعتماد ادراک شده در استفاده از سیستم های پرداخت می باشد. به منظور آزمون مدل، مدل سازی معادله ساختاری برای تحلیل داده های جمع اوری شده از 219 پاسخگو در کشور کره استفاده می شود. تحقیق حاضر، یک مبانی نظری برای دانشگاهیان و نیز دستور العمل های کاربردی برای عرضه کنندگان خدمات در رسیدگی به ابعاد امنیت سیستم های پرداخت الکترونیکی فراهم می کند.

کلمات کلیدی: سیستم های پرداخت الکترونیکی(EPS)، استفاده از EPS، تجارت الکترونیک، امنیت، اعتماد

1-مقدمه

تجارت الکترونیک(EC) بر مبنای سیستم های پرداخت الکترونیک(EPS) می باشد. از آنجا که EC برای بسیاری از شرکت ها تبدیل به یک جزء مهم عملیات کسب و کار و تجارت شده است، پرداخت الکترونیک به یکی از مهم ترین مسائل برای سرویس های مالی و کسب و کار موفق بدل گردیده است.(هسی 2001، پها و خامیتوف 2004، استروبورن و همکاران 2004، لینک و همکاران 2006، کاتلر و همکاران 2007، کاساردیاس و همکاران 2008). در مقایسه با روش های پرداخت سنتی، فنون پرداخت الکترونیک دارای چندین ویژگی مطلوب است از جمله امنیت، قابلیت اطمینان، توسعه پذیری، ناشناس بودن، مقبولیت، حریم خصوصی، کارایی و راحتی(چو و همکاران 2004، استروبورن و همکارا 2004،تسیاکیس و استفاندیاس 2005، لینک و همکاران 2006، کوتلر و همکاران 2007، کاساردیاس و همکاران 2008).EPS توجه زیادی را به خود جلب کرده و در سرتاسر دنیا مورد استفاده

قرار گرفته است. کشور هایی نظیر فرانسه، آمریکا و بریتانیا دارای سیستم های کاملا پیشرفته می باشند، این در حالی است که مناطقی نظیر کشور های حاشیه آسیا-پاسیفیک، انگیزه رشد را برای صنعت فراهم کرده اند.

تحقیق ما از کشور کره به عنوان منطقه مطالعه تجربی استفاده می کند زیرا زیر ساخت های پشتیبانی مورد نیاز برای توسعه EPS، در این کشور مناسب بوده است. کره با سرعت زیادی توسعه فناوری اطلاعات و شبکه ها را دنبال کرده و یک زیر ساخت فناوری اطلاعات در کلاس جهانی را ایجاد کرده است(آو و کافمن2008). از اواسط 1990، دولت کره، تعدادی از سیاست ها را برای توسعه و ارتقای EC به مرحله اجرایی درآورده است. در نتیجه این سرمایه گذار یهای متمرکز، کره در حال حاضر دارای یک زیر ساخت سطح جهانی برای تجارت الکترونیک است. بر طبق گزارش سالانه تجارت الکترونیک منتشر شده توسط وزارت بازرگانی کره در 2007، کل اندازه بازار EC در کره ،507.42میلیارد دلار با رشد 34.6 در مقایسه با سال قبل است. در عین حال، کره دارای یکی از بزرگ ترین آمار های سرانه مصرف اینترنت می باشد: تعداد کاربران اینترنت 34.430.000 بوده(و یا 75.5 درصد جمعیت با سن شش سال یا بزرگ تر) و به طور پیوسته در حال افزایش است. در عین حال،خرید و تراکنش های آنلاین به یک بخش مهم از زندگی برای مصرف کنندگان عادی تبدیل شده است.

انتظار می رود که بازار تجارت الکترونیک در کره طی پنج سال آینده، هر سال دو برابر شود. چون کره دومین بازار فناوری اطلاعات سریع الرشد دنیا است،EPS نقش مهمی در اجرای فعالیت های گسترده و فعالیت های مربوط به مقابله با شرایط اقتصادی در حال تغییر ایفا می کند. درحقیقت، بسیاری از برند های EPS نظیر Easycash, Easypaydirect, Inipay, iCash, eGate, eCredit, Smartpay, mypay.net, Payplusو Paymatics در طی سال های اخیر ایجاد شده اند.

اگرچه EPS خوب دارای برخی مزایا نسبت به روش های پرداخت مرسوم و سنتی است، با این حال آن ها بایستی عاری از هر گونه نقض امنیت باشند(هگارتی و همکاران 2003، لینک و همکارا 2006).گروه گارتنر گزارش کرده است که 95 درصد مشتریان در زمان استفاده از کارت های اعتباری در اینترنت تا حدودی نگران حریم خصوصی یا امنیت هستند. موسسه هریس اینتراکتیو نیز گزارش می کند که شش نفر از ده نفر شرکت کننده در نظر سنجی ترس سرقت کارت اعتباری را دارند. یک عامل کلیدی برای موفقیت EPS، امنیت می باشد، یک لازمه مهمی که در محیط تجارت الکترونیک جهانی فعلی بیش از بیش اهمیت پیدا کرده است(هرزبرگ 2003، استروبورن و

همکاران 2004، پها و خامیتوف 2004، تسیکیس و استفاندیس2005، لینک و همکاران 2006، کاتلر و همکاران 2007). تراکنش ها در تجارت الکترونیک می تواند بدون هر گونه تماس قبلی انسانی و یا ارتباطات بین فردی اثبات شده رخ دهد. داستان ها در موردتهدید های امنیت تجارت الکترونیک از رسانه ها یا شبکه های بین فردی می تواند موجب کاهش اعتماد به EPS شده و از این روی موجب می شود تا افراد به اعتماد بین فردی که در تعاملات انسان با انسان ناشی می شود روی آورند. به طور کلی، امنیت، مجموعه ی از رویه های، سازو کار ها و برنامه های کامپیوتری برای صحت سنجی و به رسمیت شناختن منبع اطلاعات و تضمین فرایند است(تئودوسیوس و جرج 2005، لینک همکاران 2006).اگرچه منابع فعلی به طور گسترده ای به جزییات فنی امنیت و اعتماد در EPS از دیدگاه بازرگانان یا عرضه کننده های خدمات EPS پرداخته اند، ادراک مصرف کننده ها از امنیت EPS، به خوبی بررسی نشده و مطالعات تجربی در این زمینه محدود هستند(لینک و همکاران 2006).

تعدادی از سیستم های پرداخت الکترونیک اخیرا در اینترنت ظهور یافته اند. اگرچه شیوه ها و مکانیسم های امنیتی متعدد برای این EPS ها طراحی شده اند، بسیاری از مسائل امنیتی هنوز حل نشده باقی مانده اند(هسی 2001، چو و همکاران 2004، دای و گراندی 2007، کاسریداس و همکاران 2008). از این روی، نیاز مبرمی به کاهش ریسک های مربوط به فرایند های تراکنش پرداخت الکترونیکی احساس می شود(تسیکاس و استفاندیس 2005). چون اکثریت کاربران EPS، با جزییات فنی EPS ناآشنا می باشند،آن ها سطح امنیت EPS را بر اساس تجربه خود با واسط های کاربر ارزیابی می کنند. از این روی به منظور جذب و حفظ کاربران پرداخت الکترونیک، بهبود ادراک مصرف کننده ها از امنیت و حفظ اعتماد مشتریان در طی تراکنش های پرداخت الکترونیک بسیار مهم است(چلاپا و پاولوف 2002، استربورن و همکاران 2004، تسیکاس و استفاندیس 2005، لینک و همکاران 2006، کاساردیس و همکاران 2008). هدف اصلی این تحقیق، بررسی تجربی عوامل موثر بر ادراک مصرف کننده ها از اعتماد و امنیت و نیز اثرات امنیت و اعتماد ادراک شده بر روی استفاده از EPS از دید مصرف کنندگان است.

در بخش بعدی، ما به مرور EPS هایی می پردازیم که در تجارت الکترونیک بنگاه با مشتری یا مشتری با مشتری وجود دارند و سپس به بررسی تحقیقات قبلی در زمینه مسائل امنیت و اعتماد در EPS می پردازیم. بخش سوم، یک مدل مفهومی اکتشافی از اعتماد ادراک شده و امنیت ادراک شده مصرف کننده ها در استفاده از EPS را

توسعه داده و در بر گیرنده فرضیات تحقیق و ساختار ها است. ما روش تحقیق و نتایج را در بخش چهارم بحث می کنیم. نتیجه گیری و اهمیت تحقیق در بخش 5مطرح شده است.

2- مبانی نظری

2-1 سیستم های پرداخت الکترونیک

وقتی تجارت الکترونیک، نیاز به خدمات پرداخت الکترونیک را برجسته تر کرد، ابزار های پرداخت مبتنی بر حساب و مبتنی بر پول نقد سنتی به عنوان یک مدل استفاده شدند. هم زمان، ابزار های واسطه نظیر پی پال در رفع برخی نیاز های جدید مصرف کننده ها و تاجران انلاین موفق بودند(دالبرگ و همکاران 2008).

پرداخت الکترونیکی در این جا به صورت انتقال الکترونیکی یک مبلغ از پرداخت کننده به دریافت کننده از طریق یک مکانیسم پرداخت الکترونیکی تعریف می شود. سرویس های پرداخت الکترونیکی، به صورت واسط های کاربر وب محور وجود دارند که به مشتریان امکان دسترسی از راه دور و مدیریت حساب ها و تراکنش های بانکی آن ها را می دهد(ویر و همکاران 2006، لیم 2008).

آمار بانکداری بین المللی از بانک تسویه حساب های بین المللی و بانک مرکزی اروپا نشان می دهد که ابزار های پرداخت مورد استفاده برای پرداخت خرید های روزانه نظیر پول نقد، چک، کارت بدهی و کار اعتباری می باشند.(لاورنس و همکاران 2002، گاون و هاو 2003، ابرازهیوچ 2004،دای و گراندی 2007، اشنایدر 2007)، که به صورت زیر می باشند:

1-پول نقد الکترونیکی: تراکنش ها از طریق مبادله پول الکترونیک تسویه می شوند

2- کارت پیش پرداخت: مشتریان از کارت پیش پرداخت برای یک مبلغ خاص با وارد کردن یک شماره کارت منحصر به فرد بر روی سایت های تجاری استفاده می کنند

3- کارت های اعتباری: یک سرور، هویت مصرف کننده ها را احراز کرده و با بانک چک می کند که آیا وجوه کافی قبل از خرید موجود است یا خیر، هزینه ها به حساب مشتری ارسال می شوند و مشتری بعدا صورت حساب هزینه ها به مشتری ارایه شده و موجودی حساب را به بانک پرداخت می کند.

4- کارت های بدهی: یک مشتری، تراز مثبت را در حساب حفظ می کند و وقتی که تراکنش بدهی انجام شد، پول از حساب کسر می شود

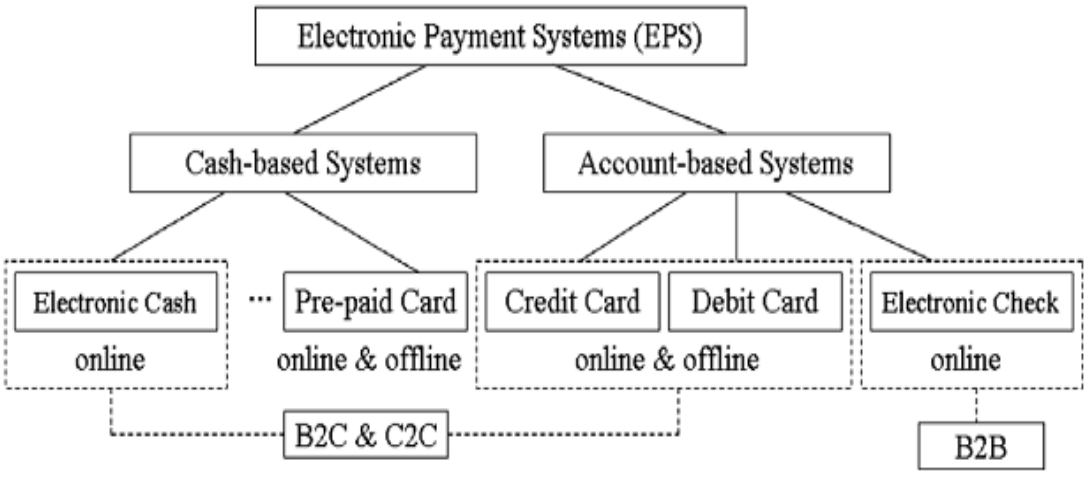
5-چک های الکترونیک: یک سازمان به طور الکترونیک تراکنش ها را بین بانک خریدار و بانک فروشنده در شکل یک چک الکترونیک انجام می دهد.

پول نقد الکترونیک، کارت های پیش پرداخت، کارت های اعتباری و کارت های بدهی به طور گسترده در تجارت الکترونیک بنگاه با مشتری و مشتری با مشتری استفاده می شود(تئودوسیس و جرج 2005) که در شکل 1 نشان داده شده است. این مطالعه بر این چهار نوع EPS متمرکز است.

2-2 سیستم های پرداخت الکترونیک در تجارت الکترونیک بنگاه با مشتری و مشتری با مشتری

2-2-1 پول نقد الکترونیک

پول نقد الکترونیک، یک روش پرداخت است که در آن یک شناسه منحصر به فرد مربوط به یک مبلغ خاصی از پول است. پول نقد الکترونیک اغلب اشاره به پول نقد الکترونیک(ای کش) یا پول نقد سایبری دارد(جوسون 2001، رایت 2002، استادلر 2002، چو و همکاران 2004). این روش به عنوان یک روش جایگزین برای استفاده از کارت های اعتباری برای خرید های اینترنتی کالا و خدمات توسعه یافته است. برای استفاده از این سیستم پرداخت، مشتریان، پول نقد دیجیتال الکترونیکی را از شرکت صادر کننده خرید می کنند(ابرازویچ 2004).سپس پول نقد از طریق کامپیوتر ها و یا سایر کانال های ارتباط از راه دور انتقال می یابد(هسی 2001). روش پول نقد دیجیتال مستلزم وجود یک سازمان برای صدور و بازخرید پول نقد می باشد. خصوصیت کم هزینه بودن پول نقد الکترونیک باعث شده است تا به یکی از مناسب ترین روش ها برای پرداخت میکرو تبدیل شود(پانراچ 1996، لاورنس و همکاران 2002، رایت 2002، کیم و همکاران 2006).



شکل 1: طبقه بندی سیستم های پرداخت الکترونیک

سیستم های پرداخت الکترونیک(EPS)، سیستم های مبتنی بر پول نقد، سیستم های مبتنی بر حساب، پول نقد الکترونیک، کارت پیش پرداخت، کارت اعتباری، کارت بدهی، کنترل الکترونیک، آنلاین، آنلاین و آفلاین، آنلاین، آنلاین و آفلاین، بنگاه با مشتری و مشتری با مشتری، بنگاه با بنگاه

2-2-2 کارت پیش پرداخت

کارت های پیش پرداخت برای یک مقدار خاص توسط یک تاجر خاص صادر شده و به کرات در تراکنش های فروشگاهی استفاده می شوند. کارت می تواند به صورت یک هدیه ارایه شود و یا به عنوان یک شیوه ساده برای انجام خرید استفاده شود. استفاده آسان و راحت، از دلایل اصلی استفاده از این کارت توسط مصرف کننده ها است. کارت پیش پرداخت معمولا برای تاجران و بازرگانان مطلوب است زیرا مشتریان تمایل دارند تا هنگام استفاده از آن، پول بیشتری خرج کنند(کنیبرگ 2002).

2-2-3 کارت اعتباری

پرداخت های کارت اعتباری از مکانیسم های کارت اعتباری افلاین نشات می گیرند(لاورنس و همکاران 2002). کارت های اعتباری رایج ترین نوع پرداخت الکترونیک هستند(هسی 2001، چو و همکاران 2004). دو مسئله مهم مربوط به روش کارت اعتباری، امنیت(استروبورن و همکاران 2004) و حریم خصوصی می باشد زیرا اطلاعات تراکنش مصرف کننده ها را می توان از طریق کارت های اعتباری پایش کرد(لادون و تراور 2001). روش کارت اعتباری شامل یک ساختار تراکنش پیچیده غیر قابل تقلیل می باشد(هسی 2001، رایت 2002). در مقایسه با سایر EPS ها، این EPS برای تراکنش های کم ارزش مناسب نیست یعنی تراکنش های کم تر از یک دلار(کالاکتوتا و وینستون 1996).

2-2-4 کارت بدهی

کارت بدهی، یکی از رایج ترین سیستم ها برای پرداخت الکترونیک است.روش کارت بدهی، ترکیبی از ویژگی های دستگاه خود پرداز با بانک داری اینترنتی می باشد. وقتی که مشتریان با یک کارت بدهی پرداخت می کنند، پول به طور خودکار از حساب بانکی آن ها کسر می شود. بر عکس با کارت های اعتباری، پول خرج شده مستقیما از

حساب بانکی برداشت می شود. بسیاری از بانک ها، یک کارت بدهی را صادر می کنند که می توان از آن در مکان هایی استفاده کرد که کارت های اعتباری پذیرفته نمی شوند. وقتی که کاربران با یک کارت بدهی پرداخت می کنند، پرداخت به صورت یک تراکنش بدهی پردازش می شود(آبرازویچ 2004).

2-2-5 خلاصه

کارت های پیش پرداخت، کارت های اعتباری و کارت های بدهی، رایج ترین روش های پرداخت الکترونیکی در تجارت الکترونیکی بنگاه به مشتری و مشتری به مشتری می باشند، در حالی که روش پول نقد الکترونیک به عنوان مکمل آن ها عمل می کند. هر روش پرداخت الکترونیک یک کار مهم را در تراکنش های تجارت الکترونیک انجام می دهد. روش پول نقد الکترونیک برای تراکنش های کم ارزش مناسب است در حالی که کارت های پیش پرداخت، کارت های اعتباری و کارت های بدهی را می توان برای بیشتر انواع تراکنش ها به کار برد، اگرچه تراکنش های کم ارزش می توانند به طور نامتناسبی پر هزینه باشد. چون هیچ سیستم پرداخت الکترونیکی وجود ندارد که کاملا در تراکنش های تجارت الکترونیک غالب باشد، هر سیستم پرداخت الکترونیک می تواند به صورت مکمل با سیستم های پرداخت الکترونیکی دیگر عمل کند. برای سیستم های پرداخت میکرو، کارایی و سرعت، مهم ترین عوامل هستند. مسائل امنیتی برای تراکنش های پرداخت الکترونیک کم ارزش بسیار مهم می باشند. برای تراکنش های با ارزش زیاد، امنیت مهم ترین مسئله می باشد و استفاده از رمز گذاری و سایر مکانیسم های امنیتی بایستی به منظور کاهش ریسک های تراکنش پرداخت التروئیکی در نظر گرفته شود.

2-3 مرور منابع در خصوص مسائل امنیت و اعتماد در EPS

به منظور شناسایی عوامل موثر بر اعتماد ادراک شده و امنیت ادراک شده مصرف کننده ها در استفاده از EPS در تجارت الکترونیکی بنگاه به مشتری و مشتری به مشتری، این بخش مروری بر منابع مربوطه داشته و یک مبانی مفهومی ارایه می شود.

از آنجا که اینترنت یک شبکه باز با کنترل غیر مستقیم انسان بر تک تک تراکنش ها است، زیر ساخت فنی که از ES و EPS پشتیبانی می کند، بایستی در برابر حملات امنیتی مقاوم باشد. حفاظت های فنی برای کاهش این نوع ریسک بایستی قبل از حل مسئله اعتماد مصرف کننده در نظر گرفته شوند. کالاکوتا و وینستون(1997) برخی از مسائل مربوط به امنیت EPS را بررسی کرده اند. آن ها خاطر نشان کرده اند که EPS بایستی در برابر

نفوذ های امنیتی مصون و مقاوم باشد و این که آسیب پذیری EPS بایستی به طور دقیق در نظر گرفته شود. امنیت تراکنش های پرداخت الکترونیک بستگی به یک سری عوامل دارد نظیر عوامل مربوط به سیستم یعنی زیر ساخت و پیاده سازی فنی(لادون و تراور 2001، لینک و همکاران 2006)، عوامل مربوط به تراکنش یعنی پرداخت ایمن بر طبق قواعد خاص و تعریف شده(هوانگ و همکاران 2007، لیم 2008) و عوامل حقوقی یعنی یک چارچوب حقوقی برای تراکنش های الکترونیک(پها و خامیتو 2004). اسلیک و بلانگر (2003) با مرور فناوری های امنیتی موجود برای EPS،از جمله فنون رمز گذاری و احراز هویت، به این نتیجه رسیدند که یک سیستم پرداخت الکترونیکی ایمن بایستی یک امنیت در برابر فعالیت های کلاهبرداری ارایه کند و از حریم خصوصی مصرف کننده ها حفاظت کند. در نهایت، رامدین(2005)، به اهمیت ارزیابی امنیت برای EPS پرداخته و بیان می دارد که یک سیستم پرداخت الکترونیکی ایمن بایستی دو مولفه زیر را داشته باشد:1-صحت، که شامل احراز هویت، پیشگیری از کلاهبرداری و حریم خصوصی می باشد و 2- قابلیت خرد شدن، قابلیت انتقال، پیشگیری از هزینه مجدد، محرمانگی پرداخت، ناشناس بودن پرداخت و قابلیت پیگیری پرداخت.

روش های تراکنش در EPS در مطالعات و منابع قبلی مورد بحث قرار گرفته اند(برای مثال، لینک و همکاران 2006، هوانگ و همکاران 2007، کوساریداس و همکاران 2008). مراحل موجود در شیوه های پرداخت الکترونیک متفاوت از مراحل موجود در سایر روش های پرداخت سنتی می باشند زیرا زیر ساخت های تراکنش، اساسا متفاوت از یک دیگر می باشند: این می تواند موجب بروز انواعی از مسائل امنیتی جدید از جمله نگرانی های مربوط به استفاده غیر مجاز و وضعیت تراکنش شود(لینک و همکاران 2006، هوانگ و همکاران 2007، لیم 2008). اگرچه یک سیستم پرداخت الکترونیک مزیت غلبه بر محدودیت های زمانی و مکانی را در مقایسه با تراکنش های افلاین سنتی دارد، ادراک مشتریان از امنیت و اعتماد به سیستم ها، اهمیت زیادی برای افزایش استفاده از این سیستم ها دارد(لینک و همکاران 2006، کاساریداس و همکاران 2008). لادون و تراور(2001) بیان داشته است که تعاملات فرایند و رویه های پیشرفته بایستی در EPS برای حل مسائل امنیتی توسعه یابند. لاورنس و همکاران(2002) نیز بیان می دارند که تعاملات فرایند اصلاح شده در EPS قادر به حذف ترس مصرف کننده ها در خصوص مسائل امنیتی مربوط به استفاده از EPS می باشد.

ارسال بیانیه های امنیتی در سایت های پرداخت الکترونیک، یک مرحله مهم دیگر است(برای مثال، ماخرجی و نات 2003، کاتلر و همکاران 2007، لم 2008). اصطلاح"بیانیه امنیت" اشاره به اطلاعات ارایه شده به مصرف کننده ها برای عملیات EPS و راه حل های امنیتی دارد. با این حال، مطالعات کمی به اهمیت بیانیه های امنیتی در EPS پرداخته اند. میازاکی و فرناندز(2000) استدلال می کنند که بیانیه های امنیتی پست شده بر روی وب سایت ها موجب افزایش شانس خرید و پرداخت مصرف کننده در اینترنت می شود. منطق و دلیلی که این فرض را تایید می کند، بر اساس مفهوم عدم تقارن اطلاعات و نقشی که آن در تصمیم گیری ایفا می کند می باشد. عدم تقارن اطلاعات اشاره به شرایطی دارد که در آن یکی از طرفین معامله یا تراکنش به همه اطلاعات مورد نیاز برای تصمیم گیری دسترسی ندارد(اکرولف 1970). این موضوع به عنوان یکی از مسائل مهم در EPS شناخته شده است. بر طبق ماخرجی و نات(2003)، دامنه و بزرگی عدم تقارن اطلاعاتی(یعنی بیانیه های امنیتی به مشتریان ارسال نمی شود)، بایستی بر ادراک مصرف کننده ها از امنیت و اعتماد در EPSس تاثیر بگذارد. فریدمن و همکاران(2002) نیز پیشنهاد می کند که ویژگی های بیانیه های امنیت، بیانیه ها و گزارشات حفاظت از داده ها و حریم خصوصی، گزارشات سیاست- امنیتی و سایر محتوی توصیفی در خصوص احتیاط های ایمنی به کاربران در ایجاد تفاسیر دقیق تر از مفهوم سیستم پرداخت الکترونیکی ایمن کمک می کند.

مصرف کننده ها به شدت به ریسک های موجود در امنیت اطلاعات و حریم خصوصی شخصی حساس می باشند. تعداد زیادی از مطالعات تجربی قبلی بر جزییات فنی حفاظت نظیر حریم خصوصی و صحت تاکید کرده اندکه برای استفاده از EPS توسط مصرف کننده ها مهم است(تسیاکیس و استفاندیس 2005، لینک و همکاران 2006، هوانگ و همکاران 200، کاساداریس و همکاران 2008). با این حال، روش های تراکنش برای احراز هویت، تصدیق و اصلاح، در EPS مهم هستند(تسیایکس و استفاندیس 2005، لینک و همکاران 2006، هوانگ و همکاران 2007، کاساداریس و همکاران 2008). فراهمی، قابلیت دسترسی و قابلیت درک بیانیه های امینتی برای تراکنش های پرداخت الکترونیکی مهم است(ماخرجی و نات 2003، کاتلر و همکاران 2007، لیم 2008). همه این سه بعد بایستی در طراحی EPS امن در نظر گرفته شوند.

بر اساس این مرور منابع، می توان یک سری عوامل موثر بر ادراک مصرف کننده ها از امنیت و اعتماد را در استفاده از EPS به سه زمینه طبقه بندی کرد: بیانیه های امنیتی، روش های تراکنش و حفاظت های فنی(شکل2).

همان طور که قبلا توصیف شد، بیانیه های امنیتی اشاره به اطلاعات ارایه شده به مصرف کننده ها در رابطه با عملیات EPSو راه حل های امنیتی دارند. حفاظت های فنی اشاره به مکانیسم های ویژه و فنی برای حفاظت از امنیت تراکنش مصرف کننده ها دارند. روش های تراکنش اشاره به مراحلی دارند که برای تسهیل اقدامات مصرف کننده ها و حذف ترس امنیتی آن ها طراحی می شوند.

3- مدل و فرضیات تحقیق

3-1 مدل تحقیق

مطالعات تجربی اندکی بر روی روابط مستقیم بین امنیت ادراک شده مصرف کننده و اعتماد ادراک شده در EPS انجام شده اند. یک مطالعه استثنای مهم، مطالعه چلاپا و پاولو (2002) می باشد. آن ها به این نتیجه رسیده اند که تراکنش های آنلاین در معرض چندین تهدید امنیتی هستند و پیشنهاد می کنند که اعتماد مصرف کننده ها به تراکنش های آنلاین تحت تاثیر امنیت ادراک شده می باشد. آن ها این فرض ها را تست کرده و یک رابطه مثبت و معنی دار را بین ادراک امنیت مصرف کننده ها از تراکنش های آنلاین و اعتماد آن ها به این تراکنش ها اثبات کردند. تدوزیس و جرج(2005) استدلال کردند که عرضه کننده های خدمات پرداخت الکترونیک بایستی اعتماد و امنیت را به عنوان عوامل مهم موثر بر استفاده مصرف کننده ها از EPS در نظر بگیرند.

تحقیقات تجربی بر روی مسائل امنیتی که بر اساس دیدگاه مصرف کننده ها می باشد، پیچیده هستند زیرا مفاهیم امنیتی، بسیار انتزاعی هستند. برای حل این مسئله، ما یک پرسشنامه نظر سنجی را با استفاده از چارچوب نظر سنجی امنیتی توسط لینک و همکاران(2006) توسعه دادیم.آن ها بر مسائل امنیتی موثر بر مشارکت مصرف کننده ها در یک روش پرداخت موبایل تاکید کرده و مفهوم امنیتی را به دو بعد طبقه بندی کردند: امنیت عینی و امنیت ذهنی. این تحقیقات، مفهوم خود را از ابعاد امنیتی عینی و ذهنی گرفته اند. در بعد ذهنی، ما شیوه های امنیتی را به صورت راه حل های منسجم در EPS در نظر می گیریم که به همه مسائل امنیتی پاسخ می دهند از جمله حفاظت های فنی، روش های تراکنش و بیانیه های امنیتی. با این حال، مشتریان عادی به سختی قادر به ارزیابی عینی راه حل های امنیتی EPS می باشند(اگر و ابرازیویج 2001). بیشتر آن ها، امنیت EPS را بر اساس واسط خود با سیستم ارزیابی می کنند. ارزیابی های ذهنی مصرف کننده ها از امنیت، اثری بر روی شیوه های

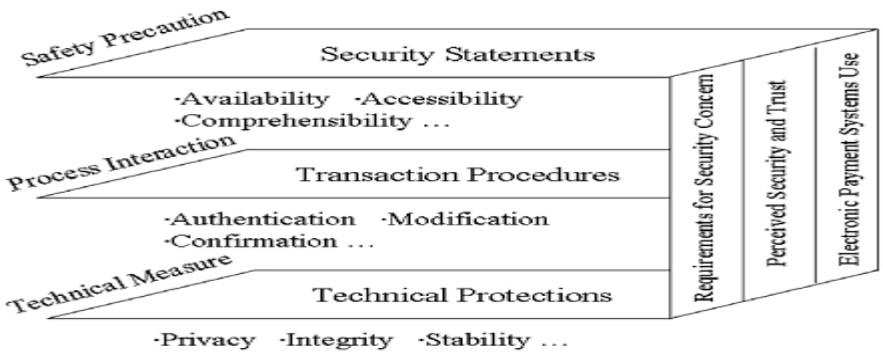
امنیتی عینی ندارد، در حالی که، سطح روش های امنیتی عینی بر ارزیابی ذهنی مصرف کننده ها از امنیت اثر دارد(لینک و همکاران 2006).

این مطالعه، یک مدل تحقیق استفاده از EPS توسط مصرف کننده را تست می کند که تحت تاثیر ادراک مصرف کننده ها از امنیت و اعتماد قرار دارد. ما امنیت ادراک شده مصرف کننده و اعتماد ادراک شده آن ها را تلفیق کرده و به یک مدل تحقیق تبدیل می کنیم با فرض این که هر دوی امنیت و اعتماد، در طی تراکنش پرداخت الکترونیک، از دغدغه های مهم مصرف کننده ها باشد. در صورتی که سیستم پرداخت الکترونیک یک محیط تراکنش ایمن را ارایه نکند، مصرف کننده ها، با تردید از سیستم استفاده می کنند و این می تواند موجب کاهش اعتماد مصرف کننده و در نهایت کاهش استفاده از سیستم می شود(گان و هائو 2003، ماخرجی و نات 2003، لینک و همکاران 2006، کاسارایداس و همکاران 2008). شکل 3، مدل تحقیق ما را بر اساس فرضیات تحقیق خلاصه سازی می کند. اگرچه برخی از عوامل امنیتی EPS شناسایی شده در این مدل در مطالعات قبلی ارایه شده است، مدل تحقیق ما، یک سری عوامل تعیین کننده و موثر بر ادراک مصرف کننده ها از امنیت و اعتماد را علاوه بر استفاده از هر دو اعتماد و امنیت ادراک شده در نظر می گیرد. همان طور که در این مدل نشان داده شده است، حفاظت های فنی، روش های تراکنش و بیانیه های امنیتی از عوامل اصلی موثر برای ادراک مصرف کننده ها از امنیت و اعتماد در استفاده از EPS می باشند.این سه عامل به طور مستقیم تعیین کننده این موضوع هستند که آیا یک مصرف کننده، یک سیستم پرداخت الکترونیک را به صورت ایمن در نظر می گیرد و این که آیا یک مصرف کننده به EPS اعتماد دارد یا خیر.

3-2 فرضیات تحقیق

3-2-1 حفاظت های فنی در EPS

حفاظت های فنی به طور کلی به عنوان اساس امنیت EPS در نظر گرفته می شوند. یک سری از مکانیسم های فنی خاص برای اطمینان از امنیت پرداخت در طی فرایند تراکنش در اینترنت استفاده می شوند(اسلیک و بالنگر 2003، لینک و همکاران 2006، کاسیرداس و همکاران 2008).



شکل 2: نمودار عوامل موثر بر امنیت ادراک شده و اعتماد ادراک شده در استفاده از EPS

حفاظت ایمنی، بیانیه ایمنی، قابلیت فراهمی، قابلیت دسترسی، قابلیت درک، تعامل روند، روش های تراکنش، احراز هویت، اصلاح، تصدیق، ملزومات مربوط به مسائل امنیتی، امنیت و اعتماد ادراک شده، استفاده از سیستم های پرداخت الکترونیک، روش فنی، حفاظت فنی

حفاظت های فنی	امنیت ادراک شده در EPS	
رویه های تراکنش	اعتماد ادراک شده در EPS	استفاده از EPS
بیانیه های امنیت		
بعد عینی پرداخت الکترونیک	بعد ذهنی پرداخت الکترونیک	

شکل3: مدل امنیت ادراک شده و اعتماد ادراک شده در استفاده از EPS

در ارتباط با این مفهوم، چلاپاو پاولوف(2002) بیان کرده اند که امنیت و اعتماد ادراک شده به طور مطلوبی تحت تاثیر حفاظت های فنی قرار می گیرند از جمله حریم خصوصی، صحت و پایداری. در صورتی که یک سیستم پرداخت الکترونیک بتواند یک تضمینی را در خصوص حریم خصوصی، صحت و پایداری ارایه کند، آنگاه، سطح اعتماد و امنیت ادراک شده مصرف کننده ها در EPS را می توان بهبود بخشید(رومدان 2005، تسیکاس و استفاندیس 2005، هوانگ و همکاران 2007) بر این اساس، ما فرض می کنیم که حفاظت های فنی احتمالا اثر مثبت بر روی ادراک مصرف کننده ها از اعتماد و امنیت دارند.

فرضیه 1: حفاظت های فنی ارتباط مثبت با امنیت ادراک شده مصرف کننده ها در EPS دارد

فرضیه 2: حفاظت های فنی ارتباط مثبت با اعتماد ادراک شده مصرف کننده ها به EPS دارد

2-2-3 روش های تراکنش در EPS

هدف اصلی روش های تراکنش، تسهیل استفاده مصرف کننده ها از EPS و حذف نگرانی در مورد امنیت EPS(لاورنس و همکاران 2002) می باشد. به منظور رفع نیاز های امنیتی مصرف کننده ها، مراحل و روش های به خوبی تعریف شده EPS بایستی تهیه شوند(هوانگ و همکاران 2007). معمولا، سه روش اصلی در طی فرایند تراکنش استفاده می شوند 1- احراز هویت هر یک از شرکت کننده ها قبل از تراکنش2- ارایه چندین مراحل مجزا به مصرف کننده ها برای تکمیل تراکنش پرداخت الکترووینک و 3- ارسال یک تاییدیه بعد از هر تراکنش برای این که مصرف کننده ها اطمینان حاصل کنند که سیستم پرداخت الکترونیک به طور موفق کار خود را انجام داده است(تسیکیس و استفاندیس 2005، هوانگ و همکاران 2007). فرضیه ما این است که روش های تراکنش اثر مثبت بر روی هر دو امنیت ادراک شده و اعتماد ادراک شده به EPS دارند.

فرضیه 3: روش های تراکنش ارتباط مثبت با امنیت ادراک شده مصرف کننده ها به EPS دارد

فرضیه 4: روش های تراکنش ارتباط مثبت با اعتماد ادراک شده مصرف کننده ها به EPS دارد

3-2-3 بیانیه های امنیتی در EPS

بر طبق گزارش ماخرجی و نات(2003)، بیانیه های امنیتی در وب سایت های EPS، یک عامل موثر بر اعتماد مصرف کننده در فعالیت های انلاین می باشند. با اطلاع رسانی و مطمئن کردن مصرف کننده ها در خصوص امنیت گزینه های پرداخت، امکان تاثیر گذاری بر ادراک مصرف کننده ها از امنیت و اعتماد به EPS وجود دارد(لیم 2008).در صورتی که مصرف کننده های معمولی از سطح امنیت تراکنش های خود آگاه نباشند، آن ها در استفاده از پرداخت های الکترونیک، مردد خواهند بود(هاگراتی و همکاران 2003، لیم 2008). تصمیم مصرف کننده ها برای استفاده از هر سیستم پرداخت الکترونیک به طور قابل ملاحظه ای تحت تاثیر کیفیت بیانیه های امنیتی موجود برای آن ها دارد. این مفهوم با نتایج گزارش شده توسط میازاکی و فرناندز(2000)تایید شده است به طوری که همان طور که قبلا گفته شد، این محققان استدلال کردند که بیانیه های امنیتی ارسال شده و پست شده در وب سایت ها موجب افزایش شانس خرید مصرف کننده در اینترنت می شود.فرض ما این است که بیانیه های امنیتی اثر مثبت بر روی امنیت ادراک شده مصرف کننده ها و اعتماد ادراک شده به EPS دارند.

فرضیه 5: بیانیه های امنیتی ارتباط مثبتی با امنیت ادراک شده مصرف کننده ها در EPS دارند

فرضیه 6: بیانیه های امنیتی ارتباط مثبتی با اعتماد ادراک شده مصرف کننده ها در EPS دارند

3-2-4 امنیت ادراک شده در EPS

امنیت ادراک شده اشاره به ارزیابی ذهنی مشتریان از امنیت سیستم پرداخت الکترونیک دارد(لینک و همکاران 2006). چون مصرف کننده ها دارای تجربه ها و انتظارات متفاوتی می باشند، آن ها می توانند نگرش های متفاوتی در قبال امنیت تراکنش های آنلاین داشته باشند. این مسئله حتی زمانی که سیستم های پرداخت الکترونیکی، تضمین هایی را با توجه به همه ابعاد ملزومات امنیتی مصرف کننده ارایه کند، صادق خواهد بود(استروبورن وهمکاران 2004). در صورتی که سطح امنیت ادراک شده در تراکنش پرداخت الکترونیک بسیار پایین است، تا زمانی که راه حل هایی برای کاهش ترس آن ها ارایه نشود بعید است که مصرف کننده وارد فرایند تراکنش شود(نسیاکیس و استفاندیس 2005). در واقع، برخی از مطالعات نشان می دهند که ادراک مصرف کننده ها از امنیت مربوط به پرداخت الکترونی، موجب تقویت تصمیم آن ها مبنی بر استفاده از EPS می شود.امنیت و اعتماد دو دغدغه مهم مشتریانی هستند که از EPS استفاده می کنند و آن ها ارتباط نزدیکی با هم دارند(گان و ها 2003،پهاو خامیتوف 2004، لینک و همکاران 2006). از این روی، ما دو فرضیه در خصوص نقض امنیت ادراک شده در رابطه با اعتماد ادراک شده مصرف کننده ها و استفاده از EPS پیشنهاد می کنیم.

فرضیه 7: امنیت ادراک شده در EPS ارتباط مثبت با اعتماد دراک شده مصرف کننده ها در EPS دارد.

فرضیه 8: امنیت ادراک شده در EPS، ارتباط مثبت با استفاده مصرف کننده ها از EPS دارد.

3-2-5 اعتماد ادراک شده در EPS

اعتماد ادراک شده مصرف کننده ها در EPS به صورت باور مصرف کننده ها مبنی بر این که تراکنش های پرداخت الکترونیکی بر طبق انتظارات آن ها پردازش می شوندتعریف می شود(تسیاکیس و استفاندیس 2005، مالات 2007). مصرف کننده ها می توانند بر اساس دانش مربوطبه پاداش های احتمالی برای اعتماد و عدم اعتماد، تصمیم منطقی بگیرند. اعتماد موجب افزایشش سود می شوددر حالی که عدم اعتماد موجب اجتناب از زیان های بالقوه می شود(لینک و همکاران 2006، کازاریداس و همکاران 2008). نگرش مصرف کننده ها در قبالEPS، مربوط به ادراک آن ها از امنیت سیستم ها است. به عبارت دیگر، ادراک مصرف کننده ها از اصول اجرای امنیت نشان دهنده باور آن ها به امنیت بوده و به این ترتیب به ادراک آن ها از اعتماد برای تراکنش های

الکترونیک کمک می کند. کنیبرگ (2002) بیان می دارد که کاربران و تاجران، تمایل زیادی برای استفاده از سیستم پرداخت غیر ایمن از یک شرکت مورد اعتماد نسبت به سیستم پرداخت ایمن از شرکت غیر قابل اعتماد دارند(صفحه 60). این نتیجه با یافته های مطالعات قبلی هم خوانی دارد(تسیکاس و استفاندیس 2005، مالات 2007) که نشان می دهد اعتماد مهم تر از امنیت است. بدون اعتماد مشتری، استفاده زیاد و چشمگیر از EPS، بسیار سخت خواهد بود. از این روی فرضیه ما این استکه اعتماد ادراک شده مصرف کننده ها به EPS بر استفاده از EPS اثر می گذارد.

فرضیه 9: اعتماد ادراک شده در EPS ارتباط مثبتی با استفاده از مصرف کننده ها از EPS دارد.

3-3 اندازه گیری

این بخش به توصیف اندازه گیری سه متغیر اصلی موثر بر ادراک مصرف کننده ها از امنیت و اعتماد EPS می پردازد.

3-3-1 اندازه گیری حفاظت های فنی

این تحقیق، سه حفاظت فنی را با استفاده از سه مقوله زیر اندازه گیری می کند: حریم خصوصی، صحت و محرمانگی(فریدمن و همکاران 2002، تسیاکیس و استفاندیس 2005، هوانگ و همکاران 2007). یک مکانیسم حفاظت از حریم خصوصی موجب می شود تا مصرف کننده ها اطمینان حاصل کنند که اطلاعات شخصی آن ها نظیر نام، آدرس و جزییات تماس، در اختیار گروه ها و طرفین دیگر قرار نمی گیرد(رایت 2002، پها و خامیتوف 2004).مصرف کننده ها تمایل دارند تا اطمینان حاصل کنند که اطلاعات ارایه شده به فروشنده ها در طی یک پرداخت الکترونیک قابل استفاده توسط سایر گروه ها نیست(سیلگ و بلامگر 2003، چاو و همکاران 2004). این حفاظت های فنی را می توان با سیاست های خالص حاصل کرد از جمله استاندارد سازی به شیوه ای که اطلاعات مصرف کننده، مورد استفاده قرار گرفته، ذخیره شده و به طور ایمن حفاظ ت شود(پیلورا 2001). برخی از مصرف کننده ها تمایلی به استفاده از EPS ندارند، زیرا آن ها می رسند که اطلاعات شخصی شان در اینترنت مورد سو استفاده قرار گیرند(کالاکوتا و وینستون 1997، رایت 2002).صحت، نشان دهنده امنیت اطلاعات پرداخت هم در طی و هم بعد از یک فرایند پرداخت می باشد(رومدان 2005). مکانیسم های صحت موجب حصول اطمینان از این می شوند که سایر طرفین و گروه ها موجب اختلاف در اطلاعات یا تغییر اطلاعات پرداخت

الکترونیکی نشوند(تسیاکیس و استفاندیس 2005، هوانگ و همکاران 2007، کاساردیس و همکاران 2008). از طریق استفاده از مکانیسم های رمز گذاری می توان به این مهم دست یافت از جمله، لایه سوکت امن(SSL) و فناوری های تراکنش الکترونیک امن(اسلیک و بلانگر 2003، داهلبرگ و همکاران 2008). مصرف کننده ها معمولا اصرار دارند که صحت اطلاعات پرداخت الکترونیک تضمین شده باشد و این که مبلغ پرداخت و سایر داده ها ثابت و بدون تغییر بماند(لادون و تراور 2001). این مکانیسم بر ادراک مصرف کننده ها از امنیت و اعتماد در استفاده از EPS اثر دارد. در نهایت، اصطلاح محرمانگی، اشاره به پیشگیری از استفاده، نفسیر و درک داده ها توسط گروه های غیر مجاز دارد. محرمانگی نقش مهمی در دست یابی به اطمینان مصرف کننده ها در EPS ایفا می کند. عوامل متعددی وجود دارند که بر محرمانگی تراکنش های الکترونیک اثر دارند از جمله نرم افزار پرداخت الکترونیک، دیتابیس های پرداخت الکترونیک، پلاتفرم های سیستم پرداخت الکترونیک و منبع توان(کالاکوتا و وینستون 1997).به علاوه، حفاظت فنی برای اثبات احراز هویت گروه ها، نظیر احراز هویت دو فاکتوری برای حفظ محرمانگی مهم است. استفاده از دو فاکتور متفاوت بر خلاف یک فاکتور، موجب ایجاد سطح بالاتری از اطمینان احراز هویت می شود(فریدمن و همکاران 2002، تسیاکیس و استفاندیس 2005).

3-3-2 اندازه گیری روش های تراکنش

این تحقیق، روش های تراکنش را با استفاده از سه فاکتور زیر اندازه گیری می کند: احراز هویت، اصلاح و تصدیق. احراز هویت روشی است که از طریق آن هویت شرکت کننده ها از طریق هویت و پسورد آن ها قبل از مشارکت در سیستم پرداخت الکترونیک تایید می شود(تسیکاس و استفاندیاس 2005، هوانگ و همکاران 2007).اگرچه احراز هویت، یک روش اولیه برای پیش گیری از نفوذ های غیر قانونی ارایه می کند، با این حال در معرض یک سری از ریسک ها و خطرات ناشی از ماهیت باز اینترنت وجود دارند. احراز هویت، یک روش مشهودی است که ارتباط مستقیم با امنیت پرداخت دارد و از این روی این بر ادراک مصرف کننده ها از امنیت و اعتماد تاثیر دارد(لادون و تراور 2001، تسیاکیس و استفاندیس 2005، کاساریداس وهمکاران 2008). اصلاح، روشی است که از طریق آن مصرف کننده ها اقدام به لغو یا اصلاح مبلغپرداختی خود و یا روش پرداخت خود قبل از تکمیل مرحله نهایی فرایند پرداخت می کنند. ارایه چنین گزینه ای می تواند به مصرف کننده ها، یک حس اعتماد و اطمینان را مبنی را بر این بدهد که آن ها بر تراکنش های پرداخت خود تا مراحل نهایی کنترل دارند(لادون و تراور

2001). تصدیق و تایید، روشی است که از طریق آن مصرف کننده ها می توانند اطمینان حاصل کنند که مبلغ پرداختی آن ها به دست فروشنده ها رسیده است(لینک و همکاران 2006). در این روش، فروشنده ها یک تاییدیه را با استفاده از پیامک، ایمیل، فکس و غیره ارسال می کنند. ارایه اطلاعات تاییدیه در خصوص یک پرداخت، بر ادراک مصرف کننده از امنیت و اعتماد به استفاده از EPS اثر دارد(رامدن 2005).

3-3-3 اندازه گیری بیانیه های امنیت

این تحقیق بیانیه های امنیت را از طریق سه فاکتور اندازه گیری می کند: قابلیت فراهمی، قابلیت دسترسی و قابلیت درک. اول، قابلیت فراهمی اشاره به اطلاعاتی دارد که از استفاده مصرف کننده ها از سیستم پرداخت الکترونیک پشتیبانی می کند(ماخرجی و نات 2003). مصرف کننده ها نیازمند اطلاعات و دانش در خصوص انواع گزینه ها و عملیات ارایه شده توسط EPS می باشند. بیانیه های ناکافی می توانند مانع از استفاده مصرف کننده از EPS شوند(لیم 2008). از این روی، یک سیستم پرداخت الکترونیک به خوبی طراحی شده بایستی بیانیه ها و گزارشات کلی را در خصوص توصیف فنی و عملکرد EPS ارایه کند یعنی 1- دستورات و گزینه های موجود در پرداخت الکترونیک 2- توضیحاتی در مورد شیوه استفاده ازیک دستور پرداخت الکترونیک و 3- توصیه هایی در خصوص شیوه پیش گیری ازخرابی در سیستم پرداخت الکترونیک(میازاکی و فرناندز 2000، تسیاکیس و استفاندیس 2005، لیم 2008). علاوه بر اطلاعاتی که به مصرف کننده ها امکان می دهند تا فروشنده های قابل اعتماد و فروشنده های غیر قابل اعتماد تفاوت قائل شوند، سایر اطلاعات نیز توسط EPS ارایه می دهند. برای مثال، یک سیستم اعتبار می تواند بر اعتماد فروشنده ها اثر گذاشته و مصرف کننده ها را تشویق به استفاده از EPS می کند. دوما، قابلیت دسترسی اشاره به راحتی یافتن گزارشات و بیانیه های مربوط به ابعاد امنیتی EPS دارد(رایت 2002، هگارتی و همکاران 2003). مصرف کننده ها نبایستی هر گونه تلاش خاص یا اضافی برای یافتن بیانیه های امنیتی کنند. آن ها بایستی یا بر روی صفحه پرداخت الکترونیک و یا سایر صفحات مربوطه قابل دسترس باشند. از این روی یک سیستم پرداخت الکترونیک به خوبی طراحی شده بایستی یافتن بیانیه های امنیتی را توسط مشتریان نسبتا آسان تر کند(کاتلر و همکاران 2007). در نهایت، قابلیت درک اشاره به شیوه ارایه بیانیه های امنیتی به مصرف کننده ها دارد(لینک و همکاران 2006). بیانیه های امنیتی بایستی به اندازه کافی برای مشتریان عادی برای درک راحت تر آن ها، صریح و ساده باشند. آن ها بایستی، توجه مصرف کننده ها

را در زمان انجام تراکنش های الکترونیکی جذب کنند(ماخرجی و نات 2003).بر همین اساس، یک سیستم پرداخت الکترونیک به خوبی طراحی شده بایستی دارای ویژگی های زیر باشد:1- بیانیه ها بایستی جامع و صریح باشند 2- بیانیه ها بایستی توجه مصرف کننده ها را جلب کند(هسی 2001، کاتلر و همکاران 2007).

4-تحلیل داده ها و نتایج

4-1 روش

ارزیابی های اندازه گیری برای اعتبار سنجی مدل استفاده می شوند. بر اساس توصیه های زیر از مطالعات قبلی برای توسعه و ارزیابی ابزار های اندازه گیری(هیر و همکاران 1998، ناوک و همکاران 2000، بالن و لانگ 1993)، مطالعه ما یک روش سه مرحله ای را در دستور کار خود قرار داده است. مرحله نخست، از طریق مروز منابع مربوطه و مقیاس ها و شاخص های متناظر انجام می شود(گافن و همکاران 2000). در مرحله دوم، مجموعه ای از گزینه های ساده برای هر ساختار ایجاد شده و از نظر پایایی و روایی محتوی ارزیابی می شود(جورسکوک و سوربوم 1993، کلین 1998).در مرحله سوم، تحلیل تاییدی جامع برای EPS با آزمون و ارزیابی مقیاس های اصلاح شده برای پایایی و روایی ساختار انجام می شود. ما هم چنین روایی افتراقی و خوبی برازش مدل تحقیق را صحت سنجی می کنیم.

4-2 توزیع پرسشنامه

این تحقیق،کشور کره را به عنوان منطقه مورد مطالعه تجربی استفاده می کند. دلیل این است که تجارت الکترونیک در کره در مقایسه با کشور های دیگر فعال تر و موفق تر است، از این روی، کره یک محل مناسب برای مطالعه بر روی استفاده از EPS می باشد.

این تحقیق یک نظر سنجی دو مرحله ای را برای آزمون فرضیات تحقیق انجام داد. اولا، قبل از انجام یک نظر سنجی رسمی، یک پیش آزمون برای رازیابی نسخه اولیه پرسشنامه نظر سنجی انجام شد. نمونه های پیش آزمون از دانشکده کسب و کار یک دانشگاه در کره بدست آمد. نمونه ها متشکل از تقریبا 30 دانشجوی لیسانس و دانشجوی ارشد بودند که همه آن ها فاقد سابقه و مهارت فنی خاص در EPS بودند با این حال از EPS همانند قبل استفاده می کردند. برخی از سولاتی که پاسخگویان قادر به درک آن ها نبودند، اصلاح شدند. از دو استاد IS خواسته شد تا سوالات را برای بهبود روایی ساختار مرور کنند. نتایج حاصل از مطالعه پیش آزمون منجر به یک

نسخه نهایی از پرسش نامه نظر سنجی شد. پاسخگویان، گزینه های پرسش نامه را با میزان موافقت خود با هر جمله رتبه بندی کردند. هر گزینه یا آیتم پرسش نامه در یک مقیاس لیکرت پنج نقطه ای امتیاز بندی شد(1= کاملا مخالف، 2=مخالف، 3- بی تفاوت 4= موافق 5= کاملا موافق. پرسش نامه دارای یک سری سوالات پیش زمینه ای با مقیاس بندی اسمی بود. این سوالات مربوط به ارایه اطلاعاتی در خصوص ویژگی های جمعیت شناختی، استفاده از اینترنت، خرید های آنلاین، شیوه های پرداخت مورد استفاده و غیره بودند.

یک پرسش نامه کاغذی ساختاری در نظر سنجی رسمی استفاده شد این نظر سنجی برای ارزیابی مدل پیشنهادی و اعتبار سنجی مجموعه روابط و همبستگی های درونی مربوط به ادراک مصرف کننده ها از امنیت و اعتماد در استفاده از EPS انجام شد. نظر سنجی با شرکت کننده ها در مقیاس بزرگ از طریق یک پرسش نامه 40 ایتمی انجام شد. پرسش نامه دارای شش بخش است: حفاظت فنی، حفاظت تراکنش، بیانیه های امنیت، امنیت ادراک شده در EPS،امنیت ادراک شده در EPSو استفاده از EPS. مجموع 1260 پرسش نامه بین اکتبر 2007 و ژانویه 2008 توزیع شدند. پرسش نامه های پرینت شده از طریق ایمیل، ملاقات های شخصی و ایمیل به افرادی که در صنایع مختلف و موسسه های اجتماعی کار می کردند از جمله مدارس، دانشگاه ها، دفاتر، موسسات تحقیقاتی و شرکت هایی که به طور تصادفی در کشور کره انتخاب شده بودند ارایه شدند. بعد از توزیع پرسش نامه های نظر سنجی، ما از دریافت کننده ها آدرس ایمیل و شماره تلفن آن ها را برای افزایش نرخ پاسخ با انجام تماس و ارسال ایمیل به شرکت کننده هایی که قادر به تکمیل پرسش نامه نبودند گرفتیم. به مظور اصلاح روش ها و اررزیابی پایاییو روایی آن ها، نظر سنجی با دستور العمل های دقیق و سختگیرانه انجام شد. از هر شرکت کننده خواسته شد تا به طور کامل پرسش نامه را پر کند. از شرکت کننده ها خواسته شد تا درجه اعتماد خود را به حفاظت های فنی، روش های تراکنش، بیانیه های امنیتی، امنیت ادراک شده، اعتماد ادراک شده و استفاده از EPS که از پرداخت الکترونیکی مربوطه با فروشندگان آنلاین انتظار داشتند اررزیابی کنند.

مجموعا، 335 پرسش نامه توسط ایمیل، ملاقات های شخصی و پست جمع آوری شد. 44 پرسش نامه به دلیل پاسخ های نامعتبر یا عدم تجربه در استفاده از EPS حذف شدند و 291 پرسش نامه برای تحلیل تجربی باقی ماند(نرخ پاسخ 23.1 درصد). نمونه ما شامل 56.4درصد مرد و 43.6 درصد زن بودند. بیشتر پاسخگویان، کاربران با تجربه EPS بودند. از حیث سن، 11.2 درصد شرکت کننده ها بین 11 و 19، 47.9 درصد بین 20 و 25

سال، 22.8 درصد بین 26 و 30 سال و 18.1 درصد بالاتر از 30 سال بودند. 72.2 درصد شرکت کننده ها از اینترنت به مدت بیش از یک ساعت در روز استفاده می کردند. 50.5 درصد از شرکت کننده ها گزارش کردند که آن ها بیش از دو خرید آنلاین در هر ماه انجام داده اند. ارزش محصولات خریداری شده به صورت انلاین بین 1000 و 10000 دلار بود. رایج ترین EPS های مورد استفاده،کارت های اعتباری، تحویل پول و حساب های مجازی بودند.

ترکیب نمونه می تواند به طور بالقوه، محدود کننده تعمیم پذیری یا کلیت بخشی نتایج باشد زیرا بیش از 80 درصد شرکت کننده ها دارای سن سی سال یا کم تر بودند(پترسون 2001).با این حال، کاربران جوان و میان سال EPS، بخش مهمی از جمعیت کاربر کره را تشکیل می دهند. بر طبق گفته لین و لو 2000، نتایج بدست آمده از تحلیل این نوع نمونه، می تواند نشان دهنده پدیده های واقعی باشد و از این روی برایند ها و نتایج مهمی را داشته باشد زیرا کاربران جوان و میان سال، معم ترین اقشار جمعیت کاربر هستند. و در نهایت این کاربران، فعال ترین مصرف کننده ها در EC در آینده ای نزدیک هستند. از این روی، نمونه را می توان به صورت معرف جمعیت کل کاربران EPS در کره در نظر گرفت.

4-3 آزمون های پایایی و روایی

4-3-1 آزمون روایی

تحلیل عاملی، ساختار اصلی در چارچوب مجموعه ای از متغیر های مشاهده شده را شناسایی می کند(میازاکی و فرناندز 2000). نرم افزار SPSS(بسته آماری برای علوم اجتماعی) در ارزیابی روایی استفاده شدند. ما اقدام به ارزیابی روایی ساختار با شناسایی مفاهیم امنیت ادراک شده و اعتماد ادراک شده کردیم. به علاوه، امتیازات فاکتور از اجزای شناسایی شده از پرسش نامه نظر سنجی رسمی استخراج شدند.

یک تحلیل عاملی اکتشافی در ابتدا به صورت چرخشی برای شناسایی معنی داری و اهمیت عوامل و فاکتور های فرضی انجام می شود(روایی همگرایی). همه مقادیر ویژه بزرگ تر ازیک می باشند و آیتم ها به ساختار های اصلی خود کاهش می یابند. در نهایت،یک تحلیل مولفه های اصلی به عنوان روش استخراج برای تحلیل عاملی تاییدی با چرخش واریماکس استفاده می شود.

جدول 1: مقدار KMO و آزمون بارتلت

شاخص کفایت نمونه گیری کیزر-میر-الکین		0.866
آزمون کرویت بارتلت	کای اسکوئر تقریبی، درجه آزادی، معنی داری،	3572.301 406 0.000

بیست و نه آیتم نظر سنجی در پرسش نامه مربوط به تحلیل عاملی بود. به منظور تعیین ساختار اصلی، ماتریس همبستگی در ابتدا برای تعیین میزان مناسبت آن برای تحلیل عاملی بررسی شد. مقادیر KMO(کیزر-میر-اولکین) برای هر یک از بیست و نه آیتم نظر سنجی بیش از 0.45 بود. به علاوه، مقدار آماره آزمون کرویت بر اساس تبدیل کای اسکوئر دترمینان ماتریس همبستگی، بزرگ بود(0.887) و سطح معنی داری مربوطه بسیار کوچک بود(0.000). همان طور که می توان در جدول 1 دید، نتیجه این است که داده ها تقریبا شامل داده های نرمال چند متغیره هستند. به علاوه، ماتریس همبستگی دارای تغییر همگام کافی برای فاکتور گیری است.

به منظور تعیین این که حفاظت های فنی، روش های تراکنش، بیانیه های امنیت، امنیت ادراک شده، اعتماد ادراک شده و استفاده از EPS، متغیر های مجزایی هستند، یک تحلیل عاملی تاییدی از طریق SPSS انجام شد. راه حل مولفه اول با استفاده از روش واریماکس با مولفه هایی که مقادیر ویژه آن ها بزرگ تر از یک بود مورد چرخش قرار گرفت که معیاری برای حفظ فاکتور است. بر اساس آزمونScree و مقادیر ویژه که بزرگ تر از یک بودند، شش فاکتور به صورت فاکتور های قابل تفسیر پذیرفته شدند. این عوامل، 60.01 درصد واریانس را توجیه کردند. جدول 2 نتایج تحلیل عاملی را نشان می دهد.

جدول 2: ماتریس مولفه چرخش یافته

Items	Component					
	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6
TECH4	.800					
TECH5	.731					
TECH2	.706					
TECH6	.662					
TECH1	.658					
TECH3	.575					
PROC4		.827				
PROC5		.768				
PROC6		.710				
PROC3		.679				
PROC2		.657				
PROC1		.629				
TRUS4			.836			
TRUS3			.795			
TRUS2			.740			
TRUS1			.682			
STAT1				.782		
STAT2				.742		
STAT4				.689		
STAT5				.620		
STAT3				.609		
STAT6				.494		
SECU2					.745	
SECU4					.725	
SECU1					.708	
SECU3					.620	
USE2						.827
USE1						.815
USE3						.706
Eigen values	3.550	3.324	3.103	2.887	2.342	2.199
% Of Variance	12.240	11.463	10.699	9.955	8.077	7.581
Cumulative %	12.240	23.703	34.402	44.357	52.434	60.015

آیتم ها	مولفه					مقادیر ویژه،	درصد تجمعی
عامل 1	عامل 2	عامل 3	عامل4	عامل 5	عامل 6	درصد واریانس،	

جدول 3: آزموت ضریب پایایی

Scales	Number of items	Alpha	Mean	Standard deviation
Technical protections	6	0.8493	4.32	0.63
Transaction procedures	6	0.8211	4.27	0.43
Security statements	6	0.7717	4,37	0.47
Perceived security	4	0.7502	4.23	0.48
Perceived trust	4	0.8737	4,33	0.62
EPS use	3	0.7727	4.21	0.45

Note: $n = 294$.

مقیاس ها	تعدادگزینه ها	آلفا	میانگین	انحراف معیار
حفاظت های فنی	6	0.8493	4.32	0.63
روش های تراکنش	6	0.8211	4.27	0.43
بیانیه های امنیت	6	0.7717	4.37	0.47
امنیت ادراک شده	4	0.7502	4.23	0.48
اعتماد ادراک شده	4	0.8737	4.33	0.62
استفاده ازEPS	3	0.7727	4.21	0.45

یادداشت:n=0.294

4-3-2 آزمون پایایی

پایایی با آلفای کرونباخ تعیین می شود که یک روش رایج برای اندازه گیری پایایی است(ماخرجی و نات 2003). نانالی (1978) بیان می دارد که برای هر تحقیق در مراحل اولیه، امتیاز پایایی یا آلفای برابر با 0.60 یا بزرگ تر کافی است. همان طور که در جدول 3 نشان داده شده است، امتیازات پایایی همه ساختار ها بیش از آستانه

تنظیم شده توسط ناناللی بود. همه شاخص ها، سطوح خوبی از پایایی را نشان دادند(بزرگ تر از 0.70). مقیاس اعتماد ادراک شده بزرگ ترین پایایی 0.8737 را نشان داد/

4-4 مدل سازی معادله ساختاری

همان طور که در منابع پیشنهاد شده است(بالن و لانگ 1993، چورسکوگ و سوربوم 1993، کلین 1998)، برازش مدل با شاخص هایی مظیر شاخص برازش تطبیقی(CFI)، شاخص خوبی برازش(GFI، هیر و همکاران 2003)، شاخص برازش نرمال(NFI) و ریشه خطای میانگین مجذورات تقریب(RMSEA، استیگر 1990) ارزیابی می شود. شاخص برازش تطبیقی شاخص برازش کلی است(گربینگ و همکاران 1993). شاخص خوبی برازشف برازش یک مدل را در مقایسه با مدل های دیگر اندازه گیری می کند(هیر و همکاران 2003).شاخص برازش نرمال، نسبت بهبود مدل از حیث برازش را در مقایسه با مدل پایه اندازه گیری می کند(هیر و همکاران 2003). RMSEA، اطلاعاتی را از حیث اختلاف درجات آزادی برای یک مدل ارایه می کند(استیگر 1990). آستانه های پذیرفته شده برای GFI, RFI, NFI, و CFI برابر با 0.90 می باشد توصیه می شود که RMSEA حداکثر 0.5 باشد و تا 0.08 قابل قبول است(گفن و همکاران 2000).

صحت مدل تحقیق با استفاده از روش های مدل سازی معادله ساختاری با AMOS 6.0 موردآزمون قرار گرفت. آماره کای اسکوئر مدل با درجه آزادی 368 درجه برابر با 686.546 بود که این نشان دهنده برازش خوب با مدل است(نسبت کم تر از 3). با این حال، چون آزمون کای اسکوئر به اندازه نمونه بسیار حساس است، ما از تعدادی شاخص دیگر برای آزمون برازش مدل استفاده کردیم. همان طور که در جدول 4 نشان داده شده است همه شاخص های RMR, GFI, AGFI, CFI, NFI, RFI, IFI, و RMSEA، در سطوح قابل قبول هستند. به طور کلی نتایج نشان داد که مدل ما، چارچوب معتبری را برای اندازه گیری امنیت ادراک شده و اعتماد ادراک شده مصرف کننده ها در EPS ارایه می کند.

5-4 فرضیات- آزمون مسیر

این بخش، نتایج آماری اندازه گیری یعنی اعتبار سنجی و آزمون فرضیات را ارایه می کند. اثرات حفاظت های فنی، حفاظت های تراکنش و بیانیه های امنیت بر روی ادراک مصرف کننده ها از امنیت و اعتماد در EPS، از طریق AMOS 6.0 ارزیابی شدند. نتایج تجربی در جدول 5 نشان داده شده اند.

همان طور که در جدول 5 نشان داده شده است، اثرات محافظت های فنی و بیانیه های امنیت بر روی امنیت ادراک شده مصرف کننده ها در EPS معنی دار است($\beta TECH = 0.360, t = 7.058, p < 0.01$ و $\beta STAT =$ 0.251، $t = 2.814, p < 0.01$). از این روی، فرضیه 1(H1) و فرضیه 5(H5) قویا توسط نتایج تایید می شود. بر عکس، اثر روش های تراکنش بر روی امنیت ادراک شده مصرف کننده ها معنی دار نبود($\beta_{PROC} = -0.069, \ t = -1.637, \ p = 0.102$)و این نشان می دهد که روش های تراکنش، عامل اصلی موثر بر امنیت ادراک شده توسط مصرف کننده ها در EPS نمی باشند. از این روی،فرضیه 3 تایید نمی شود.

نتایج نشان می دهد که حفاظت های فنی($\beta_{TECH} = 0.404, \ t = 4.968, \ p < 0.01$) و امنیت ادراک شده در EPS($\beta_{SECU} = 0.419, \ t = 3.012, \ p < 0.01$) همبستگی قوی با اعتماد ادراک شده مصرف کننده ها درEPS دارد. از این روی فرضیه 2 و 7 تایید می شوند. از سوی دیگر، اثرات بیانیه امنیت($\beta_{STAT} = 0.154, \ t = 1.239, \ p = 0.215$)و روش های تراکنش بر روی اعتماد ادراک شده مصرف کننده ها($\beta_{PROC} = 0.072, \ t = 1.189, \ p = 0.235$) معنی دار نبودند. از این روی فرضیه 4 و 6 تایید نمی شوند.

هم چنین همان طور که نتایج نشان داد،اعتماد ادراک شده مصرف کننده ها به EPS، اثر معنی داری بر روی استفاده مصرف کننده از EPS دارد($\beta_{TRUS} = 0.297, \ t = 3.835, \ p < 0.01$) از این روی، فرض 9 تایید می شود. در نهایت، اثر امنیت ادراک شده مصرف کننده ها در EPS،ارتباط مثبتی($\beta_{SECU} = 0.276, \ t = 1.814, \ p < 0.05$) با استفاده مصرف کننده ها از EPS دارد از این روی فرض 8 تایید می شود.

به طور کلی، ضرایب مسیر H1,H2,H5,H7,H9 در سطح P<0.01 معنی دار بودند و این نشان دهنده تایید این فرضیات است. ضریب مسیر H8 در سطح P<0.05معنی دار بود. و این نشان دهنده تایید فرضیه هشت است. فرضیات 3 ، 4 و 6 تایید نمی شوند.

شکل 4، خلاصه ای از نتایج را برای هر فرضیه درمدل تحقیق نشان می دهد. معنی داری مقادیر و براورد ها با خط پر رنگ نشان داده شده است. همان طور که در شکل 4 نشان داده شده است،امنیت ادراک شده مشتری در استفاده از EPS،با حفاظت های فنی و بیانیه های امنیتی تعیین می شود. هم چنین بدیهی است که امنیت ادراک شده و اعتماد ادراک شده، عوامل مهم موثر بر استفاده مصرف کننده ها از EPS می باشند. به علاوه، اثر معنی دار امنیت ادراک شده بر روی اعتماد ادراک شده مشهود بود.

5-نتیجه گیری و اهمیت تحقیق

این مقاله به بررسی مسائل امنیتی در زمینه EPSازنظر مصرف کننده ها می پردازد. این مطالعه، یک مدل تحقیق را ارایه می کند که عوامل موثر بر امنیت ادراک شده و اعتماد ادراک شده مصرف کننده و نیز اثرات امنیت ادراک شده و اعتماد ادراک شده بر روی استفاده از EPS را تعیین می کند. نتایج ما نشان می دهد که هر دو حفاظت های فنی و بیانیه های امنیتی، عوامل برای بهبود امنیت ادراک شده مصرف کننده می باشند.امنیت ادراک شده مصرف کننده ها ارتباط مثبتی با اعتماد ادراک شده مصرف کننده ها و استفاده از EPS دارد. در نهایت، اعتماد ادراک شده مصرف کننده دارای اثر مثبت بر روی استفاده از EPS می باشد.نتایج با یافته های تحقیقات قبلی هم خوانی دارد(کولنانو ارمسترانگ 1999،میازاکی و فرناندز 2000).

این مطالعه، هیچ شواهدی را در مورد وجود یک رابطه معنی دار آماری بین کیفیت روشهای تراکنش و امنیت ادراک شده مصرف کننده ها یا اعتماد ادراک شده در استفاده از EPS پیدا نکرد. مقدار براورد ها بسیار کوچک بودهو از این روی فرضیه 3 و 4 را تایید نمی کند. این نتایج با نتایج مطالعه انجام شده تووسط لادون تراور(2001)، رامدین(2005) همخوانی ندارد. یک دلیل احتمالی این است که روش های پیچیده نظیر احراز هویت و روش های ورود فازی،موجب کاهش راحتی مصرف کننده ها در استفاده از سیستم های پرداخت الکترونیکی می شود. تجربه مصرف کننده های ناراحت در روش های تراکنش موجب کاهش ارزیابی از امنیت و اعتماد مصرف کننده به سیستم پرداخت الکترونیکی می شود.از این روی، عرضه کننده های سرویس پرداخت الکترونیک بایستی نه تنها یک روش ایمن بلکه روش های راحت برای سیستم های پرداخت الکترونیک به مصرف کننده ها ارایه کنند.

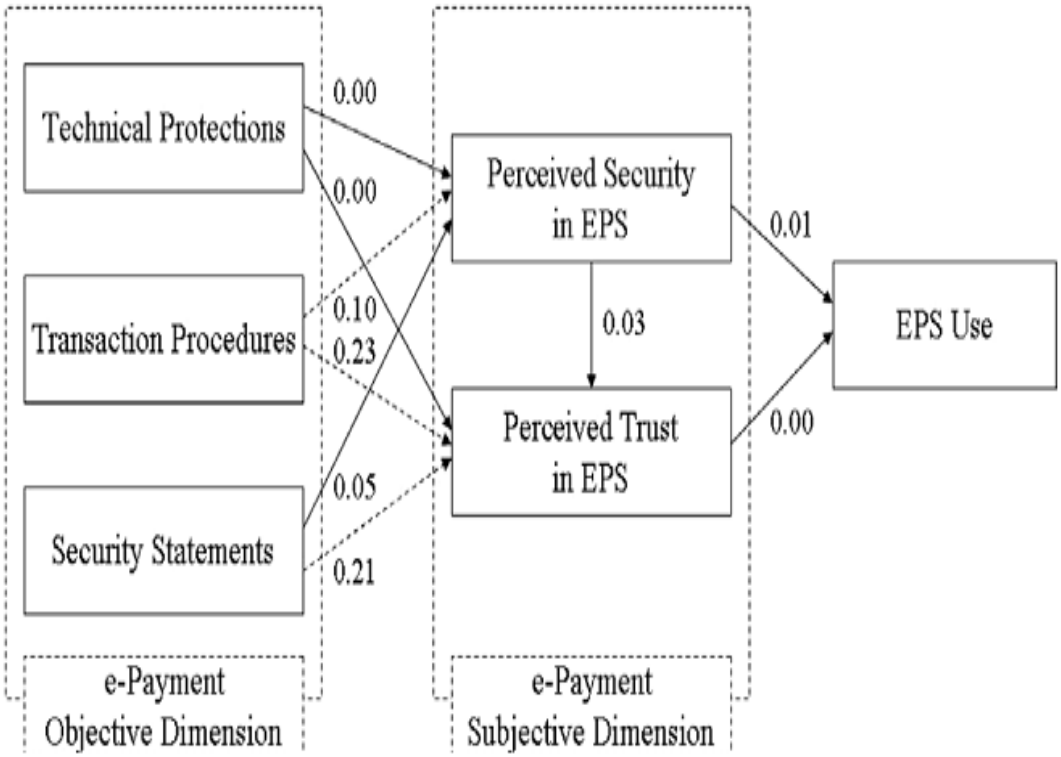
جدول 4: شاخص های برازش و نظرات برای تحلیل مدل

شاخص ها در تحلیل SEM	مدل پیش فرض	برازش داده های مدل
کای اسکوئر/نسبت درجه آزادی	1.865=368/686.546	برازش خوب (بایستی کم تر از3 باشد)
RMR (باقی مانده ریشه میانگین مربع)	0.080	برازش خوب (بایستی کم تر از 0.08 باشد)
GFI (شاخص خوبی برازش)	0.858	عدم برازش خوب(باید بزرک تر از 0.90 باشد)
AGFI (GFI تعدیل شده)	0.832	برازش خوب (باید بزرگ تر از 0.90 باشد)
NFI (شاخص برازش نرمال)	0.815	عدم برازش خوب (بایستی بزرگ تر از 0.90 باشد)
RFI (شاخص برازش نسبی)	0.796	عدم برازش خوب (بایستی بزرگ تر از 0.90 باشد)
IFI (شاخص برازش تجمعی)	0.905	برازش خوب (باید بزرگ تر از 0.90 باشد)
CFI (شتخص برازش تطبیقی)	0.903	برازش خوب (باید بزرگ تر از 0.90 باشد)
RMSEA (ریشه خطای میانگین مجذورات تقریب)	0.055	برازش خوب (بایستی کم تر از 0.80 باشد)

جدول 5: آزمون فرضیات مدل تحقیق

مسیر فرضی	براورد	خطای معیار	T	مقدار P
روش های تراکش⇐ امنیت ادراک شده در EPS	-0.069	0.042	-1.637	0.102
حفاظت های فنی⇐ امنیت ادراک شده در EPS	0.360	0.051	7.058	0.000
بیانیه های امنیت ⇐ امنیت ادراک شده در EPS	0.251	0.089	2.814	0.005
روش های تراکنش⇐اعتماد ادراک شده به EPS	0.072	0.061	1.189	0.235
حفاظت های فنی ⇐ اعتماد ادراک شده در EPS	0.404	0.081	4.968	0.000
بیانیه های امنیت ⇐ اعتماد ادراک شده در EPS	0.154	0.124	1.239	0.215
	0.419	0.139	3.012	0.003
	0.276	0.152	1.814	0.010

امنیت ادراک شده در EPS ⇐ اعتماد ادراک شده در EPS امنیت ادراک شده در EPS ⇐ استفاده از EPS اعتماد ادراک شده به EPS ⇐ استفاده از EPS	0.297	0.077	3.835	0.000



حفاظت های فنی	امنیت ادراک شده در EPS	استفاده از Eps
روش های تراکنش	اعتماد ادراک شده در EPS	
بیانیه های امنیت		
بعد عینی پرداخت الکترونیکی	بعد عینی پرداخت الکترونیک	

شکل 4: نمودار مسیر خروجی مدل تحقیق

این مطالعه، اهمیت عملی و و نظری مهم در زمینه امنیت و اعتماد در EPS دارد. این تحقیق، یک مدل نظری از امنیت و اعتماد ادراک شده مصرف کننده ها از جمله نقش آن ها در استفاده از EPS ارایه می کند. این به توجیه و توضیح روابط مستقیم بین امنیت ادراک شده، اعتماد ادراک شده و استفاده از EPS کمک می کند. نتایج ما به وضوح، نقش امنیت ادراک شده مصرف کننده ها را در ایجاد اعتماد در مشتریان و اثر مثبت هر دو امنیت ادراک شده و اعتماد ادراک شده بر روی استفاده از EPS نشان می دهد. اثراتهر دوحفاظت فنی و بیانیه امنیت بر روی

ادراک مصرف کننده ها از امنیت و اعتماد نیز تایید می شود. ادراک مصرف کننده ها از امنیت و اعتماد مفاهیم اساسی در درک ما از استفاده مصرف کننده ها از EPS است. این تحقیق با ادعا های قبلی مبنی بر این که هر دو ادراک مصرف کننده ها از امنیت و اعتماد نقش مهمی در ارتقای استفاده از EPSتوسط مصرف کننده ها دارند هم خوانی دارد. این تحقیق با ارایه مجموعه ای از مسائل امنیتی در EPS در تجارت الکترونیک بنگاه با مشتری و مشتری با مشتری به شکلی تجربی، مبنایی برای انتخاب شاخص های مناسب برای تحقیقات تجربی آینده محسوب می شود.

مطالعه حاضر پیشنهاد می کند که معرفی صرف سرویس های پرداخت الکترونیک برای جذب مصرف کننده ها به تجارت الکترونیک بنگاه با مشتری و مشتری با مشتری کافی نیست. عرضه کننده های خدمات پرداخت الکترونیک بایستی نگرانی های امنیتی مصرف کننده ها را کاهش داده و باور مشتریان را برای اعتماد به خدمات، تقویت کنند. برخی از عرضه کننده های خدمات پرداخت الکترونیک، صرفا بر روی حفاظت های فنی تمرکز می کنند و اهمیت بیانیه های امنیتی را در سیستم نادیده می گیرند. سایرین نیز به ایده" هر چه بیشتر بهتر" و یا" تا حد امکان مفصل و دقیق" را در طراحی رویه ای بر اساس ابعاد عینی امنیت تاکید دارند که به نظر می رسد ازحیث بدست اوردن اعتماد مصرف کننده ها به EPS منطقی باشد. با این حال از دیدگاه ذهنی مصرف کننده ها، این شیوه، سهولت استفاده از سرویس را نادیده گرفته و از این روی بازدهی مطلوب را ندارد. توسعه سیستم های ایمن هم در سطح عینی و هم در سطح ذهنی، برای عرضه کننده های خدمات الکترونیک بسیار مهم است. از این روی، مدیریت بایستی بر ارتقای این باور ها در میان مصرف کننده ها در زمان طراحی سیستم های امنیت تمرکز کند.

این مطالعه عاری از محدودیت نیست. اولا،اگرچه تحقیق حاضر به نتایج مهمی از نظر مصرف کننده ها دست یافته است، با این حال شامل همه عوامل موثر بر استفاده از EPSتوسط مصرف کننده ها نمیباشد. برای مثال، عواملی نظیر عملیات پرداخت الکترونیک خاص وعوامل اجتماعی و فردی که می تواند در تحقیقات آینده در نظر گرفته شود. توجه ویژه ای بایستی به عوامل انسانی، مدیریت، آموزش، آگاهی و سایر عوامل غیر فناوری برای پیشگیری از ریسک های امنیتی شود. برای مثال، برای مبارزه با سرقت هویت، آموزش می تواند در افزایش آگاهی مصرف کننده ها برای ایمن سازی داده های شخصی در دنیای فیزیکی و مجازی نقش ایفا کند. دوم، همه شرکت کننده

ها در نمونه تحقیق فعلی، در استفاده از EPS تجربه داشتند. عوامل Pre-interaction نظیر اعتبار برند، مشاوره و تجربه از منابع اطلاعات معتمد(برای مثال تبلیغات شفاهی و رسانه های سنتی) در مدل تحقیق ما در نظر گرفته نشدند. جالب است که تحقیقات آینده بر عوامل دیگری تمرکز کنند که اطلاعات دقیق تری را در خصوص امنیت و اعتماد در EPS ارایه کنند. سوما، استفاده از یک روش پرداخت الکترونیک خاص، احتمالا بر روی پاسخگویان نمونه در پاسخ های خود اثر دارد. در تحقیق ما، کارت های اعتباری و بدهی، بیش از 90 درصد استفاده از EPS را در نمونه ها توجیهکردند. اگرچه کارت های بدهی و اعتباری مستلزم روش های مشابه ای با سایر روش های پرداخت الکترونیک هستند، غالبیت این دو شیوه پرداخت لزوم تفسیر دقیق نتایج حاصله را تاکید می کند. چهارما، نمونه استفاده شده برای تحلیل تجربی، از مصرف کننده های کره ای جمع آوری شد. مسائل مربوط به پرداخت الکترونیک به طور گسترده ای در کشورهای با زیر ساخت های تجارت الکترونیکی پیشرفته تر شناخته شده اند. از این روی، مقایسه نتایج این مطالعه با نتایج مطالعات انجام شده از طریق نمونه های جمع آوری شده از سایر کشور ها جالب است. با در نظر گرفتن محدودیت های فوق، تحقیق ما یک زیر بنای مهمی برای تحقیقات آینده در شرایط ملی متفاوت محسوب می شود که در این شرایط، این تحقیقات به بررسی عوامل موثر بر امنیت و اعتماد به پرداخت الکترونیک بپردازند.