راه حل متمرکز برای انتقال الکترونیکی امن اطلاعات پرداخت به بانکها از طریق سیستم های چندگانه برنامه ریزی منابع سازمانی (ERP)

چکیده

تراکنش های مالی در یک سازمان، برای مثال پرداخت به تأمین کنندگان و حقوق کارمندان، از طریق برنامه های کاربردی چندگانه برنامه ریزی منابع سازمانی(ERP) تولید می شود و نیازمند انتقال امن به بانک ها می باشد. مدلهای پرداخت در طول سالها با تحولاتی در زمینه استفاده از روشهای پرداخت دستی، چک، کارتها، انتقال صندوق الکترونیکی (EFT) به خانه های تصفیه خودکار[1] (ACH) مواجه شده اند. مدلهای فعلی از روشهای زیرساختکلید عمومی[2] برای مراحل احراز هویت استفاده می کنند که نیاز به گواهی و تأیید مشتری و اطلاعات پرداختی دارد. مطالعه موردی حاضر یک مدل تلفیقی را پیشنهاد می کند که با استفاده از یک زیرساخت متمرکز که تبادل امن اطلاعات پرداخت از واحدهای کاری مختلف در یک سازمان را به بانک امکان پذیر می سازد، توسعه یافته است. این روش توسعه یافته از نظر مقیاس و دامنه به صرفه بوده و مجموعه ای از شیوه های استاندارد را فراهم می کند که برنامه های کاربردی چندگانه ERPتوسعه یافته برای واحدهای کسب و کار مختلفی که در مناطق مختلف جغرافیایی روی یک بستر نرم افزاری[3] امن توزیع شده اند را در حداقل زمان بازسازی و انتظار، با هم ادغام می کند. این مدل ثابت کرده که منجر به صرفه جویی در زمان و هزینه از 25٪ به 75٪ می شود و یک بستر نصب و اجرا[4] برای واحدهای کسب و کار در یک سازمان فراهم می آورد تا بطور امن با بانکهای مختلف تبادل اطلاعات پرداخت داشته باشند.

[1]Automated Clearance Houses
[2] Public Key Infrastructure (PKI)
[3]platform
[4]Plug and play platform

پردازش حقوق و دستمزد ، پروتکل انتقال فایل SSH (SFTP)، رمزگشایی داده ها، خانه های تصفیه خودکار، سیستم های ERP، حفظ حریم خصوصی (PGP)

1. مقدمه

برنامه های کاربردی ERPدر بخش های مختلف صنعتی گسترش یافته است همچون ساخت و تولید، رسانه، سازمانهای تجاری که از یک چارچوب پرداخت خودکار بواسطه ماژول هایاستاندارد حساب قابل پرداخت استفاده می کنند. این پرداخت ها یا برای فرایند حقوق و دستمزد کارمندان یا پرداخت به تأمین کنندگان اجرا می شوند. بااین حال، در بنگاه های اقتصادی بزرگتر، حجم تراکنش ها و در بیشتر موارد مبالغ درحال نقل و انتقال به میلیونها دلار می رسد، از اینرو ایمنی و امنیت مبادله داده های پرداخت با بانک، بسیار حساس می باشد. زمانی که سازمان دچار رشد ارگانی/ غیرارگانی می شود، تضمین امنیت انتقال پرداخت به بانک دچار پیچیدگی بیشتری می شود که منجر به تحول چشم انداز فناوری اطلاعات (IT) آن سازمان و حفظ زیرساخت پرداخت امن با بانک های طرف قرارداد می شود. این پیچیدگی در آنجایی چند برابر می شود که واحدهای کسب و کار متفاوت در یک سازمان، از برنامه های کاربردی ERP و IT مختلف برای تولید اطلاعات پرداخت که با بانک مبادله دارد استفاده می کنند.

تأکید این مقاله بر تضمین امنیت داده های پرداخت تولید شده از یک یا چند برنامه کاربردی ERP و به رسمیت شناختن دستورالعمل های مصوب خزانه داری و ساخت زیربناهای امن به بهترین شیوه است. این مدل امن متمرکز تلفیقی که در حال حاضر توسعه یافته و اجرا شده است، چندین برنامه کاربردی ERP را در سرتاسر واحدهای کسب و کار مختلف که در مناطق جغرافیایی متعدد پراکنده هستند را با هم ادغام می سازد تا تراکنش های بانکی را اجرا و اطلاعات پرداخت با بانک ها را بطور امن مبادله کند. این زیرساخت متمرکز از روشهای انتقال امن برای نیل به مقیاس و زمان بصرفه بهره می گیرد و می توان از آن در چارچوب های سراسری با حداقل زمان بازسازی و انتظار، استفاده کرد.

2. بررسی ادبیات این حوزه

بررسی ادبیات گسترده در این حوزه، نیاز به انتقال پرداخت امن و کارآمدکردن رویه های مختلف مربوطه را به روشنی نشان می دهد. ناکارآمدی های شایع در برنامه های پرداخت موجود و تکامل اقدامات برای کاهش خطرات قبل از پرداخت مجاز، بطور گسترده ای در این مطالعه بحث شده است. پرداخت حقوق و دستمزد شامل تراکنش های محرمانه، باید رمزگذاری شوند تا از فعالیتهای کلاهبرداری جلوگیری شود. جوریک[5] [1]، عوامل خطر بالقوه را که در پردازش پرداخت دخیل است تجزیه و تحلیل کرده و بکارگیری فنون رمزنگاری را ضروری دانسته است. دارایا و همکاران[6] [2] بر نیاز به رمزگذاری داده ها از طریق رمزنگاری برای تضمین امنیت بالا، اصرار دارند. عثمان و شاه[7] [3] بر ضرورتهای کنترل داخلی به منظور جلوگیری از وقوع تقلب و همچنین تقویت سیستم های احراز هویت، تأکید می ورزند. کورنادو- گارسیا و همکاران[8] [4] و بابو و همکاران[9] [5] از مدل زیرساخت کلید عمومی برای تضمین امنیت تراکنش ها استفاده کرده اند.

دارایا و همکاران [2]، سیستم های ERP را تجزیه و تحلیل کردند که با داده های حساس درارتباط است و نیازمند اقدامات امنیتی اضافه می باشد و اطلاعات از چنین سیستم هایی را برای امنیت بالاتر باید رمزگذاری کرد. همچنین تشخیص تقلب و نفوذ در زمان مناسب در چنین سیستم هایی ضروری است. امنیت این داده ها، از طریق بکارگیری فنون رمزنگاری تقویت شده است. این مطالعه بیشتر سعی کرده تا تشخیص فعالیتهای متقلبانه را از طریق جداول ورودی رویداد[10]، تعریف کند. محدودیت های احرازهویت معامله و تخصیص نقش ها به شکل تفکیک وظایف می تواند خطر فعالیتهای متقلبانه را محدود سازد.

ماسوچا و همکاران[11] [6]، چند مسئله فرهنگی و اجتماعی که مانع توسعه تراکنش های الکترونیکی می باشد را شناسایی کردند مثل مانع زبان، موانع قانونی کشور با فرهنگی متقابل، موانع لجستیکی، دسترسی محدود به اینترنت،

[5] Djuric
[6] Dharaiya et al
[7] Usman and Shah
[8] Coronado-Garcia et al
[9] Babu et al
[10] Event log tables
[11] Masocha et al

و بعضی مسائل امنیتی. علاوه بر این، اجرای یک سیستم ERP یکپارچه برای یک انتقال امن، مستلزم تغییرات در فرهنگ سازمانی موجود [7] است زیرا امکان دارد روش معامله سنتی در جغرافیای اجرارایج باشد.

عثمان و شاه [3] راه حل هایی را برای کلاهبرداری بانکداری الکترونیکی ارائه و تحلیل کردند. تقلب در خدمات بانکداری الکترونیکی در نتیجه سازش های مختلف در امنیت از سیستم های ضعیف احراز هویت گرفته تا کنترل های درونی ناکارآمد، رخ می دهد.

هدف این مقاله شناخت عواملی است که می تواند در تقویت سیستم های جلوگیری از تقلب در بانکداری الکترونیکی، مهم باشند. یافته های این مطالعه نشان می دهد که فراتر از فناوری، عوامل دیگری مثل تقویت کنترل های درونی، استفاده مجدد از زیرساخت های فناوری و استاندارد کردن چارچوب خزانه داری برای تأیید پرداخت ها، می تواند اطلاعات پرداخت امن به بانک ها را امن سازد.

کورنادو- گارسیا و همکاران [4]، زیرساخت کلید عمومی و ضرورت آن برای تضمین تراکنش های امن و قابلیت اطمینان بالای خدمات آن را تجزیه و تحلیل کردند. استفاده از رمزنگاری کلید عمومی، اولین شرط را برآورده می سازد، درحالیکه شرط دوم بطور سنتی با استفاده از معماری های توزیع شده[12]، برآورده می شود.به نظر بابو و همکاران [5]، بخاطر افزایش سریع در زیرساخت کلید عمومی (PKI) که برنامه های کاربردی در تراکنش های الکترونیکی متعدد را فعال کرده، ممیزی منظم سیستم گسترش یافته PKI و شناخت کارامدی این سیستم بسیار مهم است. این پژوهشگر یک رویکرد مبتنی بر عامل[13] را برای ممیزی سیستم PKI پیشنهاد می دهد. این سیستم از یک گواهی چرخه عمر تولید شده برای شیوه های احراز هویت استفاده می کند. این رویکرد مبتنی بر عامل، گزارشهای ممیزی مؤثری برای یک زیرساخت کلید عمومیارائه می دهد که مؤثرتر از ممیزیهای دستی است.

تجزیه و تحلیل ادبیات قبلی، چالش های مشخصی را در فرایند پرداخت ایجاد کرده که در ذیل فهرست شده اند. زیرساخت متمرکز پیشنهادی برای انتقال امن اطلاعات پرداخت به بانک ها از عهده چالشهای مشاهده شده برمی آید.

[12]Distributedarchitectures
[13]Agent-based approach

3. چالش های رودر روی مدل موجود

الف. اقدام به کلاهبرداری در خلال تراکنش های پرداخت

بنگاه هایی که از چارچوب های ERP بهره می برند، داده های مربوطه را با بانک مبادله می کنند. این تبادل اطلاعات با بانک با استفاده از فایلی انجام می شود که شامل جزئیات پرداخت، مقدار، واحد پول و اعتبارات حساب بانکی می باشد. بیشتر مواقع این داده های منتقل شده مستعد اقدامات کلاهبرداری یا بواسطه تغییر شماره حساب یا تغییر مقدار انتقالی می باشد.

ب. پردازش دستی ناکارآمد

بخش قابل پرداخت حساب در یک سازمان، نقشی حیاتی در تبادل اطلاعات پرداخت تأمین کنندگان یا کارمندان با بانک، ایفا می کند. فرایند پرداخت و تأییدات بعدی می تواند با استفاده از برنامه های کاربردی ERP بطور خودکار انجام شود و اگر بطور دستی صورت گیرد زمان قابل ملاحظه ای طول می کشد. تحقیق گیت پوینت[۱۴] انجام شده توسط تیپالتی[۱۵] [9]، نشان می دهد که 72 پاسخ دهنده بیش از 5 ساعت در هفته وقت صرف تنظیم دریافت کنندگان، انجام و صدور پرداخت ها، حل مسائل مرتبط با پرداخت، و اجرای سایر هماهنگی های مرتبط با پرداخت ها می کنند. این نظرسنجی علاوه براین تخمین زده که 48٪ پاسخ دهندگان یا گزارش های پرداخت را دستی به بانک ارسال کرده اند یا از اطلاعات چارچوب های ERP بهره گرفته اند. بعد از این فرایند، ارتقاء و روزآمدکردن داده ها، یک کار دستی می شود که نه تنها خطر امکان تقلب را افزایش می دهد بلکه همچنین هماهنگی داده ها را دشوار می سازد. این شیوه های دستی مستعد خطا و سوءتعبیر هستند.

پ. تراکنش های غیراستاندارد از طریق درگاه های پرداخت

چهار تا از پنج بنگاه بخاطر عدم وجود فرایندهای پرداختی استاندارد دارند فعالیتهایشان را در معرض ارائه نادرست اطلاعات پرداخت قرار می دهند [10]. این سازمانها با سطح بالای پیچیدگی متحمل تکثیر هزینه های عملیاتی و

[14]Gate point Research
[15]Tipalti

تراکنشی هستند. بنابراین علاقه رو به رشدی برای کنترل ها وجود دارد و این مستلزم یک زیرساخت متمرکز با پایه امن برای مبادله داده های پرداخت با بانک می باشد.

ت. روابط و تراکنش های بانکداری چندگانه

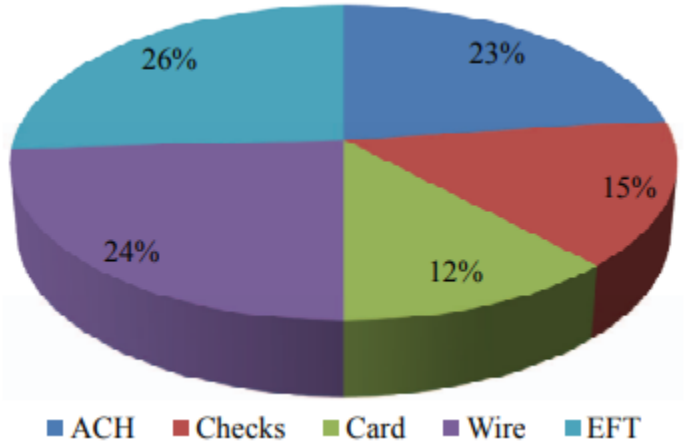
پرداخت های بانک به بانک و قابلیت اتصال به بانک[16]با مسائلی مواجه هستند درخصوص چارچوب های واگرای شبکه های ERP چندگانه که تراکنش ها را از بانک های مختلف به هم مرتبط می کنند. این شبکه پرداخت در محیط های بانکداری چندگانه، قویتر و پیچیده تر است. گزارش ارائه شده توسط سانگارد[17]توضیح می دهد که این پیچیدگی باعث شده تراکنش های کسب وکار 25 ٪ سازمانها با بیش از 10 بانک مدیریت پول نقد سروکار داشته باشد، 23٪ سازمانها بیش از هزاران حساب بانکی را مدیریت کنند [11]. درحالیکه 89٪ سازمانها، فعالیتهای کسب و کارشان را در سرتاسر کشورهای مختلف گسترش داده اند، این خدمات بانکداری بین المللی برای بیش از 55٪ فعالیتهایی که درآمدی بالغ بر 1 میلیون دلار به بار می آورند به تراکنش های بانکداری الکترونیکی متصل شده اند. از کل تراکنش هایی که بطور بین المللی صورت می گیرد، 29٪ خدمات بانکداری با گزارش هک شدن داده ها، خدمات جعلی و سوء تعبیر داده ها مواجه بودند [11]. فرصتها برای امنیت و تفسیر دقیق داده ها توسط سازمانها تشخیص داده نمی شود تا تهدیدات امنیتی کاهش یابد.

4. حالت های مختلف پرداخت

اصلی ترین روشهای پرداخت، چک های الکترونیک، خانه های تصفیه خودکار (ACH) و انتقال صندوق های الکترونیکی (EFT) هستند [12]. مطالعه انجام شده توسط سانگارد روی پرداخت های بانک به بانک براساس تجزیه و تحلیل 400 متخصص خزانه داری و امورمالی، نشان می دهد که 15٪ از پاسخ دهندگان بیشتر از چک های کاغذی استفاده می کنند تا روشهای پرداخت رایج مثل کارت های اعتباری/ بدهی ، ACH و EFT. این سازمانها

[16] The B2B Payments and Bank Connectivity
[17]SunGard

هنوز از چک هایی استفاده می کنند که با خطرات وخیم کلاهبرداری و تقلب مواجه هستند [11]. شکل 1، سهم استفاده غالب از روشهای پرداخت را نشان می دهد.



شکل 1. مرسوم ترین روشهای پرداخت [11]

الف. چک

یک تجزیه و تحلیل از نظرسنجی انجام شده توسط انجمن متخصصان امورمالی[18]، چک را برجسته ترین روش پرداخت می شناسد که درمعرضکلاهبرداریو مسبب اتلاف بیشترین مقدار دلار در سال 2014 بوده است. مناسبات بانکیبرای مبارزه با این زیان ها، اصلاح و تحول به راه حل های دیجیتال را با سرعتی کندتر، آغاز کرده است [13]. حداقل کردن استفاده و اعتماد به چک، سوءتعبیر و کلاهبرداری را در فرایندهای دستی کاهش می دهد [14].

پرداخت مثبت[19] یک ابزار تشخیص خودکار است که توسط بانک های پیشرو برای شناسایی فعالیتهای جعلی از طریق تأیید اعتبار شماره حساب، جزئیات مالی، شماره های چک از روی فهرستی از شماره های چک مجاز صادر شده توسط بانک لحاظ شده است.

[18]Association for Finance Professionals
[19] Positive pay

ب. ACH

کارACH، کنترل سازگاری جریان پرداخت و کاهشارائه نادرست اطلاعات چک با استفاده از رکوردهای ACH برای پردازش پرداخت به کارمندان، بازگانان، و سایر ذینفعان مربوطه می باشد. ACH، حجم وسیعی از تراکنشات اعتباری و بدهی را مدیریت می کند [15].

ج. EFT

یک فایل پرداخت الکترونیک منفرد از طریق تلفیق سیستم های ERP متفاوت و فرمت های مختلف EDI با پرداخت های چندگانه، داد و ستد می کند.

5. امنیت در انتقال فایل

تراکنش پرداخت مالی از یک برنامه کاربردی ERP توسط یک بخش قابل پرداخت حساب از سازمانی شروع می شود که ملزم به تبادل منابع مالی با سایر سازمان ها یا واحدهای کسب و کار از طریق بانک به عنوان یک واسطه، می باشد. این فایل که با بانک مبادله می شود می بایست رمزگذاری شده و بعد از تأیید پرداخت توسط شخص مسئولتعریف شده در هیئت مدیره آن سازمان، تولید شود. این شخص مجاز برای اجرای تراکنشات پرداخت مالی یا تأییدها، ممکن است زمان بیشتر و بررسی موشکافانه تری در اجرای تأیید اتخاذ کند. اگر این زمان بیشتر از حد معین شود، ممکن است این تراکنش مالی شروع نشود یا یک فرایند تأیید با تأخیر ممکن است باعث رد پرداخت درحال پردازش شود [16].

الف. روشهای اجتناب از ریسک های پرداخت

روشهای ذیل که در ادامه فهرست بندی شده اند می توانند تقلب را در خلال انتقال اطلاعات پرداخت به بانک کاهش دهند.

• پرهیز یا حداقل کردن استفاده از کاغذ برای کسب تأیید یا مبادله اطلاعات پرداخت.

• بهبود و تاکید بر مجازبودن، از طریق یک فرایند "جداسازی وظیفه" مقرر برای دسترسی به داده ها و تأیید جواز پرداخت از جانب افرادی که مشخصاً مجوز دارند.

• بکارگیری سیستم پرداخت خودکار در جایی که از دسترسی انسان به فایل پرداخت مبادله شده با بانک جلوگیری می شود.

• مشخص کردن یک روش تأیید برای پرداخت های الکترونیکی به عنوان آخرین مرحله در پورتال بانک به مجرد اینکه فایل توسط بانک دریافت می شود. این تأیید، مستلزم توافق رسمی بین بخش خزانه داری و بانک برای گشایش پرداخت به ذینفع آنطور که در فایل پرداخت ذکر شده، می باشد.

برای غلبه بر این مسائل مطرح شده، این مطالعه مدلی را پیشنهاد می کند که درحال حاضر توسعه یافته و برای رسیدگی به انتقال پرداخت های الکترونیکی با بانک های مختلف در یک بستر نرم افزاری امن، اجرا شده است.

6. مدل پیشنهادی

فایل پرداخت که بطور امن با بانک به اشتراک گذاشته می شود، تضمین می کند که هیچ جعل یا ارائه اطلاعات نادرستی در داده های مالی تراکنش شده نمی تواند رخ دهد. مطالعه حاضر، یک مدل زیرساخت متمرکز پیشنهاد می کند برای همساز کردن واحدهای تجاری مختلفی که از برنامه های کاربردی متعدد ITبرای اجرای تراکنشات بانکی استفاده می کنند. این زیرساخت متمرکز هماهنگ با سازمان های مختلف عمل کرده و از دستورالعمل های کلی برای مدیریت خزانه داری و از یک زیرساخت فنی ویژه برای تحویل اطلاعات پرداخت درمیان بانک ها، پیروی می کند. این زیرساخت طوری چارچوب بندی شده تا به دستورالعمل های ذیل دست یابد.

• یک خط مشی منفرد برای تأیید و جواز پرداخت، امضاء شده و پرداخت صورتحساب گنجانده شده در برنامه ERP، آزاد می شود.

• فرایند تأیید پرداخت براساس بهترین شیوه های دستورالعمل های خزانه داری سازمان، طراحی شده است.

• گشایش پرداخت ها به بانک ها، با توجه به دستورات سازمان ها در خصوص sum seethes، توازن مالی و عناصری برای نشانه گذاری و تأیید.

• مهر و موم داده ها برای پیشی گرفتن از گم شدن در انبوه اطلاعات پرداخت

• رابط های امن به و از چارچوب های ERP برای داد و ستد رکوردهاینشان دار و رمزگذاری شده

• کانال های پولی امن و مبتنی بر ارزش که با انبوه گیج کننده رکوردهای پرداخت مقابله می کنند.

• تاریخچه پردازش و مسیرهای ممیزی، تمام مراحل پرداخت، از جملهتاریخ گذاری ها، مشتریان و مشخصات تغییرکرده را شامل می شود.

• تأیید نهایی پرداخت روی پورتال بانکداری به محض اینکه اطلاعات پرداخت بطور موفقیت آمیز با بانک ها مبادله شود صورت می گیرد.

شی و ثورایسینگهام [16]، اعتبار مدلهای پردازش پرداخت را که شامل امنیت با فنون احراز هویت در انتقال داده ها می باشد، تأییدکرده اند. روند پرداخت خودکار از طریق این چارچوب، تضمینی است برای اجتناب از مداخله دستی در فرایند پرداخت، به این ترتیب خطرات تغییر فایل یا فعالیت های کلاهبرداری و تقلب کاهش می یابد.رمزگذاری داده ها و اقدامات اتصال امن در فرایند پرداخت، شامل بکارگیری کلیدها و تأییدگواهی و تأیید اعتبار مجدد برای تبادل و مبادله اطلاعات پرداخت در تمام درگاه های مختلف است. این کار امنیت و حذف کلاهبرداری را در زمان مبادله اطلاعات با بانک، تضمین می کند.

الف. ویژگی های سیستم پرداخت خودکار

صرفنظر از فرایندی که با سیستم های پرداخت سروکار دارد، سازمان باید از این زیرساخت امن استفاده کند که ویژگی های خاصی دارد از قبیل:

• سیستم امن برای اطمینان از تعریف و تخصیص صحیح نقش ها به گروه مجاز دارای اختیار و تفکیک وظایف.

• روند خودکار، یعنی عدم دسترسی دستی به فایل پرداخت به منظور حداقل کردن خطر کلاهبرداری یا ارائه اطلاعات نادرست که ممکن است درنتیجه تغییر جزئیات پرداخت بعد از ایجاد داده های پرداخت از برنامه ERP، بوجود بیاید.

• توسعه امن برای انتقال فایل اطلاعات پرداخت از طریق متن سند های خودکار از یک برنامه کاربردی ERP به بانک.

• به محض اینکه فایل پرداخت به بانک ارسال شد، تأییدیه ای از داده های پرداخت به افراد دارای صلاحیت مربوطه فرستاده می شود. توصیه می شود که یک متن برجسته امنیتی اضافی گنجانده شود که وقتی داده های پرداخت توسط بانک دریافت شد، فرد مجاز بتواند وارد پورتال بانک شده و پرداخت ها را مشاهده کرده، تأیید کند و متوجه شود.

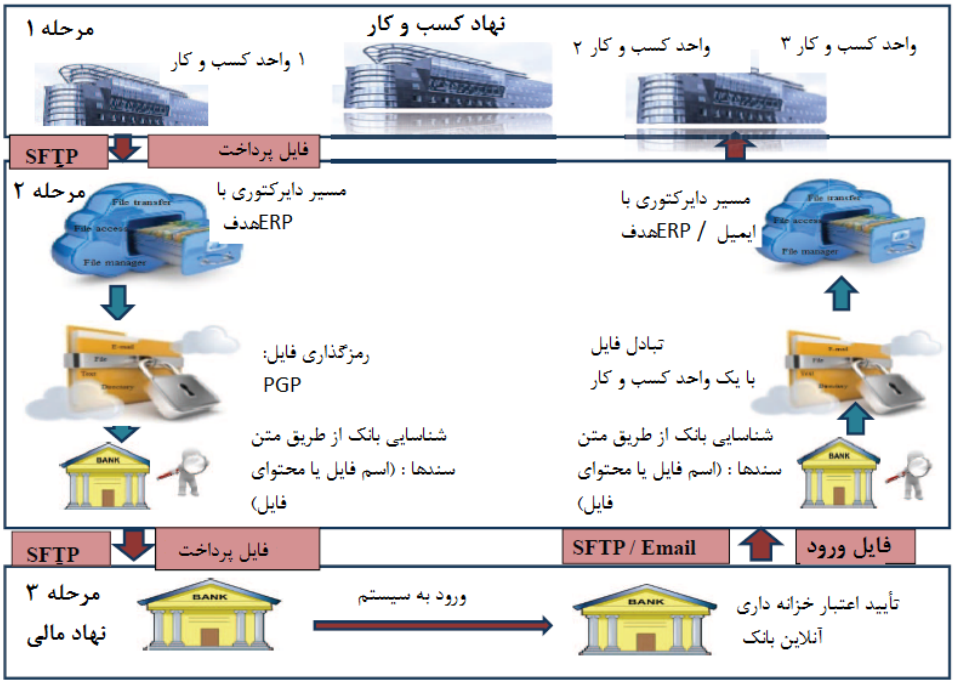
• سازگاری سریع اجازه استفاده مجدد از این راه حل را با حداقل زمان انتظار می دهد.

ب. زیرساخت پرداخت خودکار

افزایش تراکنشات باعث شده که بخش های ممیزی شرکت ها در رسیدگی به حساب مشتریان برای بررسی جریان های پرداخت و همچنین شناسایی امکان اقدامات کلاهبردارانه، با وضعیت بغرنجی دست به گریبان باشند. قبل از شروع فرایندهای تراکنش پرداخت، فایل های مرتبط با حسابها برای خزانه داری در یک سیستم ERP، قابل دسترسی می شوند. احتمال تهدید برای دزدی داده ها مشهود است زیرا این داده ها برای مدتی طولانی حتی قبل از شروع تراکنش در یک سیستم ERP یا یک شبکه ذخیره شده اند. مناسب ترین رویکرد، حفظراهبردی برای حذف کلاهبرداری از طریق رایانه ای کردن کامل این روند است نه استفاده از تأییدیه های پرداخت کاغذی،و نیز محدود کردن سقف بازه زمانی داده هایی که در خلال فرایندهای تراکنش روی کاغذ یا یک دایرکتوری شبکه ناامن ذخیره شدند.

مدل حاضر، یک ساختار کاملاً خودکار را با بالاترین میزان کنترل از طریق داده های رمزگذاری شده درنظر می گیرد که بانک ها و نهادهای تجاری مختلف را بواسطه یک شبکه واحد و امن به یکدیگر متصل می کند. معمولاً فناوری شبکه سوئیفت[20]طوری اتخاذ شده تا ساختارهای خزانه داری و مالی شرکت ها را درون یک محیط تجاری تعریف شده به هم مرتبط کند. در غیاب شبکه سوئیفت یا سیستم های مالی بانکی، از یک پروتکل SFTP رمزگذاری شده برای انتقال امن داده ها و فایل ها، استفاده می شود. در صورتی که یک SFTP در دسترس باشد، این فرایند خودکار مستقیماً داده های پرداخت را با بانک مبادله کرده و مانع هرگونه دسترسی دستی و امکان کلاهبرداری می شود.

این امنیت با تولید خودکار یک فایل روی شبکه که هیچ کس اجازه دسترسی به داده هایش را نداردتقویت می شود. این چارچوب امن نیازمند تأیید اعتبار قدرتمند برحسب رسیدگیبدون خطا بوده و کاملاً خودکار است. تراکنش های امن پرداخت ها و مبادله با بانک در یک فرایند سه مرحله ای بصورتی که در شکل 2 نشان داده شده است انجام می شود. این فرایند سه مرحله ای از تمام فرایند پرداخت مرتبط با حقوق و دستمزد یا پرداخت تأمین کنندگان در یک سازمان، مراقبت می کند.



شکل 2: راه حل متمرکز برای ERP مختلف یکپارچه برای یک تراکنش مالی امن

[20]SWIFT NET technology

مرحله 1- تولید پرداخت خودکار:اجرای پرداخت توسط بخش حسابداری با استفاده از برنامه کاربردی برنامه ریزی منابع سازمانی (ERP) و فایل اطلاعات پرداخت، تولید شده و بطور خودکار در یک سرور امن ذخیره می شود که دسترسی به این سرور با مجوز محدود، کنترل می شود.

مرحله 2- انتقال امن فایل از طریق رمزگذاری داده ها: فایل ها در این مرحله در بازه های زمانی معین معمولاً هر 10 دقیقه، با استفاده از یک وظیفه برنامه ریزی شده و یک اتصال پروتکل انتقال فایل SSH[۲۱] (SFTP) به یک سرور رمزگذاری، انجام می شود.

سازوکار انتقال فایل امن: وارد کردن و بیرون کشیدن فایل ها[۲۲] از طریق متن سندها (اسکریپت های) خاصی توسط اتصال پروتکل انتقال فایل SSH (SFTP) انجام می شود که باید فایل از درون درگاه های مختلفی عبور کند. این اتصال بین واحدهای کسب و کار محلی مختلف و سرور رمزگذاری مرکزی و نهایتاً با بانک توسط یک SFTP ایجاد شده است. تعاریف این دایرکتوری بین واحدهای مختلف و سرور رمزگذاری مرکزی بطور هوشمندانه ای تعریف و هماهنگ شده است تا انتقال داده ها بین واحدهای کسب و کار و زیرساخت امن بدون مداخله صورت گیرد و بطور شفاف ردیابی شود. این زیرساخت هم اجازه وارد کردن و هم بیرون کشیدن فایل را می دهد چرا که هم برنامه های ERP و هم سرور رمزگذاری فایل در یک شبکه سازمان قرار دارند. برای ایجاد یک لایه امنیتی اضافه یک سیستم انتقال فایل امن (با ترکیب کلید خصوصی و کلید عمومی) ایجاد شده است که بستگی دارد کدام طرف این داده ها را دارد وارد می کندیا برمی دارد.

SFTP یک پروتکل شبکه است که دسترسی به فایل، انتقال فایل و مدیریت فایل را در هر جریان قابل اعتماد از داده ها، فراهم می کند. این پروتکل اجازه طیف وسیعی از عملیات های از راه دور روی فایل ها را می دهد که باعث می شود این پروتکل بیشتر یک پروتکل سیستم فایل از راه دور باشد. مزایای استفاده از پروتکل SFTP عبارت است

[21]SSH File Transfer Protocol
[22]The push and pull of files

از بازخوانی وقفه های انتقال، فهرست های دایرکتوری، و حذف فایل از راه دور. امنیت پروتکل های SFTP از طریق بکارگیری زیرسیستم های نسخه پروتکل SSH در دو مرحله، افزایش یافته است. سرور SFTP روی پروتکل 2 SSH یک بسترنرم افزاری وابسته نیست و از اینرو مشتری که بخواهد با سرور SSH 2 مرتبط شود باید از مسیر اتصال به سرور SFTP آگاه باشد. کاربر این پروتکل را با یک کلید خصوصی/ عمومی تأیید می کند و استفاده از کلید خصوصی تنها مخصوص این کاربر است. سروری که به کاربر متصل می شود یک نسخه از کلید عمومی را دارد و زمانی که کاربر با کلید خصوصی وارد می شود، سرور از طریق یک کلید عمومی رمزگذاری شده از طریق یک دایرکتوری دردسترس، کاربر را به چالش می کشد. این کلید خصوصی کاربر، قابلیت رمزگشایی کلید ارسال شده توسط سرور را دارد در نتیجه دسترسی را فراهم می کند.

برای امنیت بیشتر، فایل پرداخت با استفاده از استانداردهای رمزگذاری صنعتی مثل حفظ کامل حریم خصوصی[۲۳] (PGP)، رمزگذاری شده است. بیشتر بانک ها روش رمزگذاری PGP را پذیرفته اند و از آن استفاده می کنند.

حفظ کامل حریم خصوصی (PGP) یک برنامه رایانه ای رمزگذاری و رمزگشایی داده هاست که حریم خصوصی رمزنگاری شده و احرازهویت برای ارتباطات داده ای را فراهم می کند.PGP غالباً برای ثبت نام، رمزگذاری و رمزگشایی متن ها، ایمیل ها، فایل ها، دایرکتوری و کل پارتیشن بندی دیسک استفاده می شود تا امنیت ارتباطات ایمیل را افزایش دهد. به مجرد اینکه این کلیدهای رمزگذاری شده برای فایل ها منقضی[۲۴]شوندبه طور خودکار از طریق بازبینیتأییصحتبازتولید می شوند.این سیستم تأیید صحت، امنیت را در تراکنش های پولی، تداوم کسب و کار، صرفه جویی در وقت و بهبود امنیت تضمین می کند. در این مدل پیشنهادی، کلید رمزگذاری خصوصی توسط سازمان نگهداری شده و کلید عمومی با بانک به اشتراک گذاشته می شود. این کار یک لایه امنیت ارتقاء یافته اضافیایجاد می کند.

[23] Pretty Good Privacy
[24] expire

مرحله 3 انتقال فایل به بانک، ورود به سیستم پرداخت و تأیید خزانه داری:

در این مرحله، فایل اطلاعات پرداخت به بانک منتقل می شود و تأییدات اضافی از خزانه داری سازمان مستقیماً به پورتال آنلاین بانک فرستاده می شوند.

این فرایند با رمزگذاری فایل بعد از اینکه به بانک منتقل شدند آغاز می شود. بااین حال، یک واحد کسب و کار ممکن است با یک یا چند بانک کار کند. این متن‌سندها طوری طراحی شده اند یا می توانند مجدداً طوری تنظیم شوند که مقصد فایل ها (بانک/ واحدهای کسب و کار) بر اساس نام یا محتوا شناسایی شود و به درگاهی منتقل شوند که فایل ها را در بازه های زمانی منظم به بانک ارسال می کند. این انتقال فایل به بانک با استفاده از پروتکل انتقال میزبان به میزبان[۲۵] کاملاً خودکار انجام می شود.

معمولاً اگر سازمانی با یک بانک واحد کار می کند این اتصال امن از قبل موجود هست و به سرعت می توان آن را برای سایر نهادها و واحدهای کسب و کار که شاید بخواهند با همان بانک معامله کنند افزایش داد. این اتصال با بانک را می توان برای سایر نهادها با استفاده از تعریف هوشمندانه فایل های پرداخت گسترش داد. به این ترتیب این مدل انگیزه ای ایجاد می کند برای یکی کردن حساب های بانکی و بازشناسی شرکای بانکی مخصوصاً زمانی که یک سازمان در حال گذر از فرایند ادغام (یکی شدن دو یا چندسازمان) و مالکیت است، هزینه های سربار و هزینه های عملیاتی را کاهش می دهد.

این راه حل پیشرفته قادر است روشهای مختلف پرداخت را مدیریت کند، دستورالعمل های خزانه داری را استاندارد کرده و قواعد تفویض اختیار بر اساس الگو را در برنامه ERP به عنوان خط مشی های سازمان/ واحد کسب و کار تعریف کند. به این ترتیب این زیرساخت خودش را به عنوان یک راه حل استاندارد عرضه می کند که امنیت فرایند پرداخت ایجاد شده از چند واحد کسب و کار را هماهنگ می سازد و تضمین می کند که اطلاعات پرداخت بدون هیچ مداخله دستی با بانک به اشتراک گذاشته می شود.

[25]Host to host transfer protocol

مدیریت فایل ورود به سیستم: به محض اینکه مسیر فایل ها به بانک مشخص شد، امکان درخواست پردازش اطلاعات فایل از جانب بانک به منظور تصدیق اینکه آیا فایل بدون هیچ خطایی پردازش شده یا خیر، میسر می شود. فایل ورود به سیستم را می توان به منظور تأییداعتبار متقابل و اتخاذ اقدامات اصلاحی در مورد خطاهای داده اصلی به یک فهرست توزیع در نهاد کسب و کار هدایت کرد.

پ. رعایت زمان اجرا برای این مدل

این مدل پیشنهادی برای تنظیم اتصال بین اولین نهاد و بانک زمان صرف می کند با اینحال زمان مورد نیاز برای تنظیم اتصالات اضافی برای واحدهای کسب و کار یا نهادهایی که در مراحل بعد ملحق می شوند بطور نمایی[۲۶] کاهش یافته است. خطوط زمانی ثبت شده در جدول 1 و 2 در خلال اجرای این مدل در منطقه آمریکا جایی که چندین واحد کسب و کار در یک سازمان از ایالات متحده، کانادا و چند کشور از آمریکای جنوبی بخشی از این توسعه بودند، رصد می شد.اجرای این مدل به سایر شرکت های گروهی تعمیم داده شد و با موفقیت در جداولزمانی رصدشده مشابه با نهادهای مختلف در آمریکای شمالی، اروپا و آسیا، آزمایش شد.

این جداول زمانی در جدول زیر منحصر به ارزیابی فنی، مسائل فنی از جمله آزمایش و پیاده سازی های فنی بعدی برای ساخت زیرساخت امن، می باشند. زمان لازم برحسب ساعت برای تنظیم این اتصال برای اولین بار و سپس بسط آن برای نهادهای بعدی در جدول 1 فهرست شده و در شکل 3 با نمودار ترسیم شده است. جدول 2 و شکل 4 ، مقایسه هزینه های اکتشافی و فنی را در راستای خطوط زمان اجرا در خلال تنظیم اولین اتصال و اتصالات بعدی نشان می دهند. هزینه اکتشافی، جمع زمان صرف شده توسط یک واحد کسب و کار برای کشف و ارزیابی بهترین راه حل فنی ممکن برای مبادله اطلاعات پرداخت با بانک و نهایی کردن فرایند پرداخت و رویه های اداری با بانک طرف قرارداد می باشد. زمانی که صرف اجرای راه حل فنی برای یک نهاد شده است را به عنوان یک هزینه فنی برای تجزیه و تحلیل درنظر می گیرند.

[26] exponentially

جدول 1

TIME DISTRIBUTION TO SETUP MODEL (HOURS) AUTHOR, 2016

	1st Entity	2nd Entity	3rd Entity	4th Entity	5th Entity
Exploration	70	50	35	25	25
SFTP between ERP (Step 1) and Business units	120	15	15	14	13
Encryption PGP (Design and test)	75	8	8	8	6
Scripts to scan the files	15	4	4	3	3
Discussion with Banks (Including tests)	120	70	48	32	32
Solution development	15	8	6	6	6
Infrastructure Maintenance	5	1	1	1	1
Security Approval	5	1	1	1	1
Provisioning of servers	4	1	1	1	1
Total Hours Required	429	158	119	91	88

جدول 2

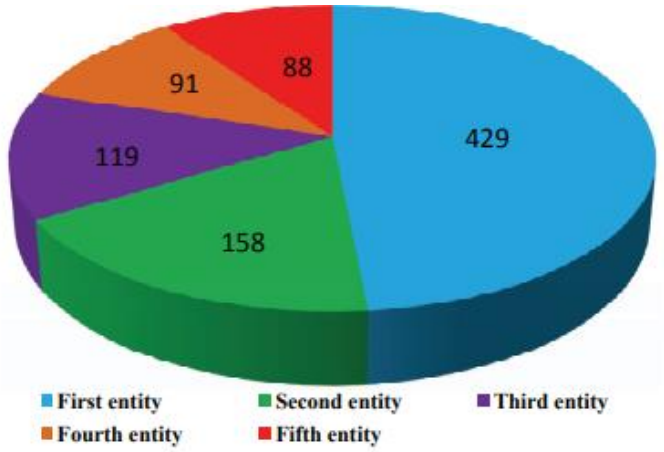
COST INCURRED FOR SETTING UP THE CONNECTION(AUTHOR, 2016)

	Exploratory Time (Hours)	Technical Time (Hours)	Total Time (Hours)	Implementation time lines (Months)
Entity /Business Unit 1	190	239	429	180
Entity /Business Unit 2	120	38	158	45
Entity/Business Unit 3	83	36	119	45
Entity/Business Unit 4	57	34	91	45
Entity/Business Unit 5	57	31	88	45

معمولاً تنظیم هر فرایند انتقال فایل جدیدی بین یک نهاد کسب و کار و بانک در کنار تعریف دستورالعمل های خزانه داری، مقدار معینی زمان می گیرد که ممکن است از 2 ماه تا یک سال طول بکشد. این زمان صرف اجرای فرایند ارزیابی گسترده و بحث امکان سنجی راه حل با بانک ها و بطور داخلی در میان سازمان IT می شود. بااینحال، از طریق این زیرساخت پیشنهادی، این زمان کم را می توان به حداقل رساند چون که این زیرساخت درحال حاضر در دسترس است.این مسئله در مورد سازمانی که درحال بازسازی و فرایند ادغام و مالکیت است، بسیار حساس می باشد.

جدول 2 این حقیقت را نشان می دهد که کل زمان تنظیم اتصال برای اولین نهاد بیشتر است اما یک بار که این مدل پیشنهادی برای جغرافیای مختلف بسط یافت، طبق اصل نظریه منحنی یادگیری و مقیاس پذیری، کارایی به ارمغان می آید و زمان اجرا کاهش می یابد.کاهش در هزینه اجرا و بهبود جداول زمانی اجرای راه حل، در شکل 4

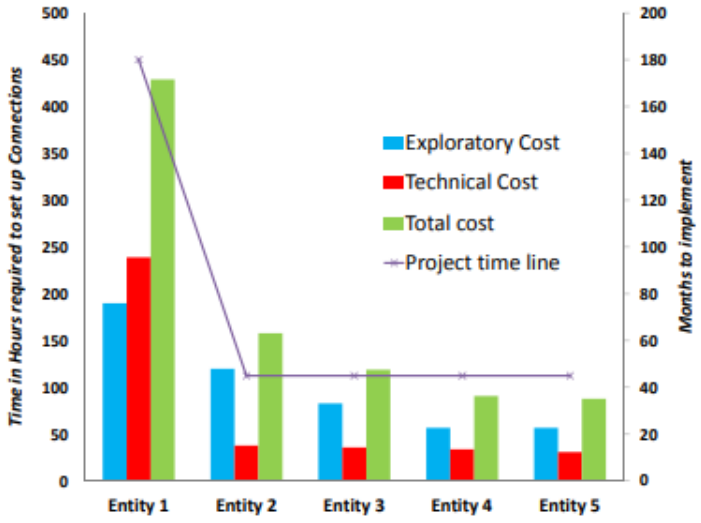
نشان داده شده است. هزینه در اینجا مستقیماً متناسب با زمان درنظرگرفته شده و به عنوان هزینه اکتشافی و فنی نمایش داده شده است.



شکل 3. کل ساعات موردنیاز برای تنظیم تراکنش ها (مؤلف، 2016)

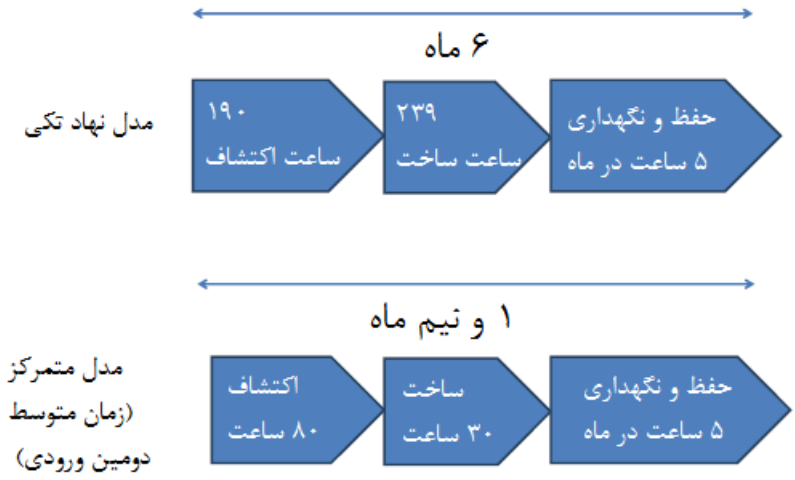
ت. مزایای اجرای این مدل

این مدل پیشنهادی، برنامه های کاربردی ERP متعدد را روی یک زیرساخت امن یکپارچه می سازد تا تراکنش های بانکی را رد و بدل کند و مزایای کمی و کیفی مختلفی نسبت به مدلهای زیرساخت کلید عمومی دارد. زمان اکتشاف برای تنظیم یک اتصال، کاهش یافته و بنابراین زمان اجرای فنی برای دومین نهاد همانطور که در شکل 2 نشان داده شده است جلو می افتد. علاوه براین، آموزش اجرای پروژه ها به نهادهای جدید تعمیم داده می شود که این امر زمان اجرای پروژه را برای هر نهاد جدیدی که به این بسترنرم افزاری ملحق شود به اندازه 25٪ کاهش می دهد. یک بار که زیرساخت امنیت و دستورالعمل های خزانه داری پیاده سازی شوند، نهادها یا واحدهای کسب و کار جدید که بعداً بخشی از این مدل می شوند از مزایای آن می توانند مجدداً بهره مند شوند. تهدیدات امنیتی به حداقل رسیده اند زیرا چارچوب کلی درون فایروال (دیواره آتش) سازمان عمل می کند و فایل داده های پرداخت با استفاده از کلید خصوصی رمزگذاری شده که توسط سازمان نگهداری می شود.



شکل 4. صرفه جویی هزینه نسبت به جدول زمانی پروژه (مولف، 2016)

پس این مدل توصیفی، امنیت داده ها (را از طریق یک کارخانه رمزگذاری) مدیریت می کند، به اقتصاد مقیاس می رسد و می تواند برای نهادهای کسب و کار مختلف در سرتاسر مناطق جغرافیایی متفاوت با فرایندهای استاندارد شده تکرار شود درعین حال اجازه اصلاحات موردنیاز قانونی ویژه آن منطقه را نیز می دهد. این مدل به اقتصاد برحسب محدوده نیز نیل کرده است زیرا همان راه حل را می توان در خلال بسط قلمروها در کسب و کار از طریق ادغام و مالکیت با حداقل زمان مصرفی، گنجاند.



شکل 5. مزایای هزینه ای و زمان بندی مدل متمرکز برای انتقال پرداخت (مؤلف، 2016)

این مدل امن با تضمین تناسب بین نام گذاری فایل پرداخت و ساختار پوشه برای ایجاد تمایز بین هر نهاد و بانک، از نظر فنی برنامه های ERP مختلف را برای نهادهای کسب و کار متفاوت یکپارچه می سازد. یک بار که اتصال امن بین سیستم های SFTP و ERP ایجاد و مستقر شد، آن را می توان برای یک نهاد کسب و کار جدید دیگر و سیستم ERP آن، بدون هیچ زمان انتظاری از نو ساخت. حفظ و نگهداری چارچوب های ITبعد از پیاده سازی، زمان چندانی نمی برد و این هزینه برای هر نهاد جدیدی که به این بستر امن ملحق شود توزیع می شود.

7. نتیجه گیری

این مدل زیرساخت متمرکز پیشنهادی، برنامه های کابردی ERP مختلف را که توسط واحدهای کسب و کار متعدد درون یک سازمان روی یک بستر امن بکار برده می شوند تا اطلاعات پرداخت را با بانک مبادله کنند، با هم یکپارچه می سازد. استفاده از پروتکل انتقال فایل امن و فناوری های رمزگذاری روی زیرساخت مرکزی، انتقال فایل امن به بانک را میسر می کند. به علاوه این راه حل از تراکنش های بانکی پشتیبانی کرده و دستورالعمل ها را با توجه به پرداخت ها از طریق یک خانه تصفیه خودکار یا پرداخت مثبت طی یک روال امن با پرهیز از اقدامات کلاهبردارانه، منتقل می کند. حلقه عبور اطلاعات در سراسر این بانکداری، با تبادل اطلاعات استاندارد که امکان سفارشی سازی در تمام نهادهای کسب و کاررا دارند، تکمیل می شود.این مدل اجازه صرفه جویی در هزینه، چابکی در اتخاذ دستورالعمل های خزانه داری محلی و وقفه ناچیز را برای تعمیم فنی این راه حل به یک نهاد یا واحد کسب و کار جدید می دهد.

References

[1] Z. Djuric, "Ips secure internet payment system," in *International Conference on Information Technology: Coding and Computing (ITCC05)*. Canada: IEEE, 2005, p. 425 430.

[2] K. Dharaiya, K. Shah, A. Lokegaonkar, and S. Jadhav, "Fraud detection and security for erps with sensitive data," *International Journal for Innovative Research in Science & Technology*, vol. 1, no. 10, pp. 261 – 262, 2015.

[3] A. Usman and M. Shah, "Critical success factors for preventing e-banking fraud," *Journal of Internet Banking and Commerce*, vol. 18, no. 2, pp. 2 – 14, 2013.

[4] L. Coronado-Garcia, C. Hernandez-Lopez, and C. Perez-Leguizamo, "A uniqueness verifying public key infrastructure based on autonomous decentralized system architecture," in *International Symposium on Autonomous Decentralized Systems*. Athens: IEEE, 2009, pp. 1 – 6.

[5] P. Babu, M. Sivakumaran, and N. Dhavale, "Auditing public key infrastructure systems: An agent based approach," in *World Congress on Nature & Biologically Inspired Computing (NaBIC)*. Coimbatore: IEEE, 2009, pp. 1632 – 1635.

[6] R. Masocha, N. Chiliya, and S. Zindiye, "E-banking adoption by customers in the rural milieus of south africa: A case of alice, eastern cape, south africa," *African Journal of Business Management*, vol. 5, no. 5, pp. 1857 – 1863, 2011.

[7] M. Srivastava and B. Gips, "Chinese cultural implications for erp implementation," *Journal of technology management & innovation*, vol. 4, no. 1, pp. 105 – 113, 2009.

[8] M. Adham, A. Azodi, Y. Desmedt, and I. Karaolis, "How to attack two-factor authentication internet banking," in *17th International Conference*. Berlin Heidelberg: Springer, 2013, p. 322 328.

[9] C. Amit. (2016) 4 reasons to automate your ap processes. [Online]. Available: http://www.itproportal.com/2016/02/05/4-reasons-to-automate-your-ap-processes/

[10] E. Holley. (2014) Corporates taking too much payment risk warns sungard. [Online]. Available: http://www.bankingtech.com/219602/corporates-taking-too-much-payment-risk-warns-sungard/

[11] SunGard. (2014) Sungard b2b payments and bank connectivity study: Innovations to overcome complexity-driven fraud exposure and cost increases. SunGard. [Online]. Available: https://www.sungard.com/solutions/corporate-liquidity/campaigns/Global-Connectivity-Messaging-Study-Whitepaper.aspx

[12] A. Phulia, M. Sharma, and D. Kumar, "Role of online banking in economy," *International Journal of Research*, vol. 1, no. 7, pp. 1039 – 1044, 2014.

[13] ACFE. (2010) Report to the nations on occupational fraud and abuse. ACFE. [Online]. Available: http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/rttn-2010.pdf

[14] O. Sobko, "Fraud in non-cash transactions: Methods, tendencies and threats," *World Applied Sciences Journal*, vol. 29, no. 6, pp. 774 – 778, 2014.

[15] CEBP, *Business-to-Business EIPP: Presentment Models and Payment Options*. Herndon, VA: CEBP, 2001.

[16] W. She and B. Thuraisingham, "Security for enterprise resource planning systems," *Information Systems Security*, vol. 16, no. 3, pp. 152 – 163, 2007.