EasyChair Preprint

№ 7141

Investigating Security Methods in Electronic Payment

Mahbubeh Fattahi Bafghi and Sima Shariatmadari

December 4, 2021

بررسی روش‌های امنیت در پرداخت الکترونیک

محبوبه فتاحی بافقی[1]، سیما شریعتمداری[2]

[1] دانشجوی کارشناسی ارشد دانشگاه آزاد اسلامی واحد بافق،
Mahbube.fatahi33@gmail.com

[2] دکترا دانشگاه آزاده اسلامی واحد یزد
S.shariat@iauyazd.ac.ir

چکیده

پرداخت الکترونیکی بعنوان یکی از دستاوردهای عرصه فناوری اطلاعات و ارتباطات، نقش بسزایی در رونق حوزه تجارت الکترونیکی واقتصاد هرکشور دارد. آنها بخش حیاتی زیرساخت اقتصادی و مالی یک کشور هستند. عملکرد خوب آنها در انتقال امن و به موقع وجوه مهمترین اثر آنها در عملکرد کلی نظام اقتصاد می‌باشد. امروزه با گسترش روز افزون معاملات الکترونیک، سیستم‌های پرداخت الکترونیکی نیز طراحی شده است که امکان پرداخت الکترونیک وجه در همان لحظه را به مشتری می‌دهد.امنیت و اعتماد لازمه ایجاد سیستم هان پرداخت الکترونیک است. راهکار های امنیتی متعددی در پرداخت الکترونیک مطرح بوده و هست. در این مقاله به بررسی تهدیدات امنیتی و روش‌های ارتقا امنیت سیستم‌های پرداخت می‌پردازیم . این مقاله درک نسبتا جامعی از چگونگی ارتقا امنیت سیستم‌های پرداخت را در اختیار خوانندگان قرار می‌دهد.

کلمات کلیدی

پرداخت الکترونیک،سیستم‌های پرداخت ،ارتقا امنیت،پروتکل امنیتی، مکانیزم امنیتی

۱- مقدمه

سیستم‌های پرداخت الکترونیکی عبارتند از: ارسال پرداخت‌ها برروی یک شبکه عمومی برای به دست آوردن کالا و خدمات. سیستم‌های پرداخت الکترونیک، سیستم‌های نرم افزاری و سخت افزاری را به گونه ای در کنار هم قرار می‌دهند،که در نتیجه آن، مشتریان می‌توانند بابت محصول خریداری شده و یا خدمت ارایه شده وجه خود را پرداخت نمایند، . اطلاعات و آمار بیانگر این است که استفاده از پرداخت الکترونیک به سرعت در حال گسترش است اما با وجود رشد افزایشی استفاده از روش‌های پرداخت الکترونیک و همچنین مزایای غیر قابل انکار آنها، استفاده از روش‌های سنتی از سوی کاربران ترجیح داده می‌شودکه دلیل عمده آن نگرانی کاربران از مسئله امنیت در این سیستم‌هاست .

امنیت اطلاعات فرایندی است که سازمان از طریق آن، سیستم‌ها، تجهیزات و شبکه‌های در برگیرنده اطلاعات حیاتی را حفاظت کرده و ایمن می‌کند. پرداخت از طریق شبکه‌ها به خصوص اینترنت امنیت بالایی می‌طلبد، زیرا ارسال داده‌ها و اطلاعات مالی از قبیل: شماره کارت اعتباری، شماره حساب، ارسال اطلاعات محرمانه مالی، ارسال کد رمز و کلمه عبور و هزاران اطلاعات محرمانه دیگر نگرانی‌های زیادی به دنبال می‌آورد و این خود دلیل موجهی برای اهمیت بالای روش‌های ایجاد امنیت و انواع مختلف سیستم‌های پرداخت امن است.

در ابتدای این مقاله به توصیف ملزومات سیستم‌های پرداخت می‌پردازیم سپس عوامل برقراری امنیت و تهدیدات امنیتی که این عوامل را به خطر می‌اندازد را بیان می‌کنیم و در پایان به ارائه چند نمونه از پرکاربردترین راهکارهای ارتقا امنیت در دو حوزه مکانیزم و پروتکل‌های امنیتی می‌پردازیم و سپس آنها را از جهت برآورده کردن ملزومات سیستم پرداخت الکترونیک بررسی می‌کنیم.

۲- ملزومات اساسی سیستم‌های پرداخت الکترونیکی

۲-۱- جلوگیری یا پیگیری خرج دوباره

یا باید از خرج دوباره پول توسط کاربران جلوگیری شود و یا اگر از یک پول مشخص بیش از یک بار استفاده شد باید فرد خاطی قابل شناسایی و پیگیری باشد.

۲-۲- تقلب ناپذیری

یعنی تا حد امکان از انجام تقلب در هر قسمت سیستم جلوگیری شود.

۲-۳- ظرفیت اتمی

علاوه بر ملزومات اساسی ذکر شده ظرفیت اتمی نیز به عنوان یکی دیگر از موارد حائز اهمیت در ملزومات سیستم‌های پرداخت به شمار می‌آید. اگر شبکه سرویس دهنده سیستم پرداخت به هر دلیلی در حین انجام پروتکل دچار ایراد شود، برخی مشکلات از قبیل مفقود شدن پول، انکار دریافت کالا از سوی مشتری و یا عدم تحویل کالا از سوی فروشنده حتی پس از دریافت وجه، امکان پذیرخواهند بود.

۲-۴- کاستن از محاسبات کلید عمومی

باید در اینگونه سیستم‌ها حتی الامکان از محاسبات کلید عمومی اجتناب شود و یا تعداد محاسبات وقت گیر و پر هزینه آن مانند تولید امضا را تا حد ممکن کاهش داد.

۲-۵- امکان تایید برون خط

حتی الامکان واسطه هیچ‌گونه راست آزمایی را به صورت برخط انجام ندهد. زیرا در زمان انجام تراکنش با محدودیت عرض باند مواجه هستیم.

۲-۶- کاستن از تبادل پیام

تعداد پیام‌های ردو بدل شده بین عناصر دخیل در اینگونه سیستم‌ها به خصوص بین کاربر و فروشنده باید به حداقل برسد.

۲-۷- کاهش ظرفیت حافظه

حتی الامکان باید از کمترین تعداد متغیرهای ثابت و دائمی که باید در حافظه ذخیره شوند، استفاده گردد.

۲-۸- گمنامی

هویت افرادی که در تجارت الکترونیک شرکت می‌کنند نباید قابل پیگیری باشد و یا دست کم تامین هزینه پیگیری آن برای افرادی عادی مقدور نباشد.

۲-۹- عدم انکار

این خاصیت بیان می‌کند که اگر پیامی از هریک از طرفین ارسال شود باید شواهدی در آن موجود باشد که نشان دهد این پیام از یک فرد خاص ارسال شده و این شواهد به گونه‌ای باشند که وی نتواند ارسال پیام را انکار کند.

۲-۱۰- قابلیت خرد شدن واحدهای مالی

حتی الامکان واحدهای مالی بکار رفته در سیستم پرداخت قابلیت خرد شدن به مبالغ کوچک تر را نیز داشته باشند.

۲-۱۱- توسعه پذیری

تعداد کاربران سیستم نباید توسط سرویس دهندگان که عمده فعالیت را بر عهده دارند محدود شود و افزودن کاربر به شبکه نباید از کارآیی آن بکاهد.

۳- عوامل لازم برای برقراری امنیت

استاندارد X.800، ۵ عنصر زیر را لازمه برقراری امنیت می‌داند :

۳-۱- محرمانگی

پنهان کاری، مخفی کاری یا محرمانگی یعنی وقتی پیغامی از طرف فرستنده برای گیرنده ارسال می‌شود، در طول مسیر جریان یافتن پیام، افراد دیگر به غیر از گیرنده نتوانند از محتوای پیام آگاهی یابد.

۳-۲- تصدیق هویت

تصدیق هویت یا تأیید هویت به معنی آن است که اگر مؤلفه ای بخواهد با مؤلفه دیگر ارتباط برقرار کند، هریک از آنها نیاز دارد هویت طرف دیگر برایش به اثبات رسیده باشد. هویت سنجی جواب این پرسش است که آیا فرستنده–ی‌درخواست یا جواب دهنده به درخواست همان شخص یا مؤلفه ای است که ادعا می کند.

۳-۳- مجوزدهی

مجوز دهی یعنی یک مؤلفه که هویت آن برای سرویس دهنده مشخص شده، تا چه اندازه از نظر این سرویس دهنده، معتبر است و مجوز دسترسی به چه اطلاعاتی را دارد .

۳-۴- صحت

درستی یا صحت به این معنی است که اطلاعاتی که فرستنده برای گیرنده ارسال می‌کند در طول مسیر یا در هر جای دیگر دست خوردگی پیدا نکند و عوض نشود. به عبارت دیگر باید روش‌هایی را بدست آورد که صحت اطلاعات ارسال شده از طرف فرستنده برای گیرنده را تضمین کند.

۳-۵- عدم انکار

عدم انکار یعنی اینکه اگر فرستنده پیامی را فرستاد در آینده نتواند منکر ارسال آن شود و در این صورت گیرنده پیام تضمین کند که اگر درخواستی از طرف

فرستنده ارسال شده و او آن را انجام داده باشد، آنگاه فرستنده نمی‌تواند منکر قضیه شود.

۴- تهدیدات امنیتی در پرداخت الکترونیکی

تهدید امنیتی اشاره به حملاتی دارند که در آنها فرد حمله کننده ، بدون تحت تاثیر قرار دادن منابع سیستمی یا با تغییر در منابع سیستم و یا با تحت تاثیر قرار دادن عملکرد سیستم سعی درگردآوری و استفاده از اطلاعات را داردکه از جمله آنها می‌توان به موارد زیراشاره کرد:

۴-۱- جعل هویت

این حمله وقتی رخ می‌دهد که یک موجودیت غیرمجاز خودش را به جای موجودیت مجاز جا زده و ارتباطی را شروع کند.

۴-۲- ارسال دوباره پیام

این حمله اشاره به وضعیتی دارد که شخص حمله کننده، یک تکه داده معتبر و بدون اشکال را در اختیار گرفته و سعی می کند آن را چندین و چندبار ارسال نماید.

۴-۳- استراق سمع

این حمله بدین معناست که حمله کننده توانسته به صورت غیر مجاز به اطلاعاتی که نباید دسترسی داشته باشد دست پیدا کند .

۴-۴- تغییر پیام

در این وضعیت شخص حمله کننده در میانه یک مسیر ارتباطی قرارگرفته و پیام تحت ارسال را پس از دریافت و تغییر، دوباره برای گیرنده ارسال می‌کند.

۴-۵- منع سرویس

هدف در این حمله، از کار انداختن توان سرویس دهی یک سرویس دهنده است. به این معنی که شخص حمله کننده با ارسال بیش از حد درخواست‌های واهی، مجالی را برای سرویس دهی درست برای سرور باقی نمی‌گذارد.

۴-۶- حملات رمز نگاری

یک مدل حمله برای تحلیل رمز است. همچنین اگر حمله کننده بتواند کوچکترین اطلاعاتی را از متن آشکار یا کلید بدست آورد این حمله موفق در نظر گرفته می‌شود. توسط این اطلاعات، دشمن می‌تواند برای بازیابی کلید امنیتی مخفی که برای رمزگشایی استفاده می‌شود، تلاش کند.

۴-۷- فیشینگ

در این حمله کاربر اطلاعات شخصی، کلمه عبور و همچنین اطلاعات مالی محرمانه را در اختیار فرد هکر قرار می‌دهد. در این فرآیند اطلاعات در قالب فرم‌ها و با عناوین مختلف از جمله بانک، مؤسسه های وابسته به دولت و غیره برای افراد مورد نظر ارسال می‌شود و آنان بدون اطلاع از اینکه فرم دریافتی جعلی است، ناآگاهانه اطلاعات محرمانه مورد نظر را درون آن وارد و ارسال می‌نمایند.

۴-۸- فیمینگ

حمله نفوذگر به منظور تغییر ترافیک وب سایت به یک وب سایت جعلی دیگر است. در این بخش از سوء استفاده، با دستکاری DNS سرویس دهنده توسط فردهکر، کاربر به به تصور اینکه وارد سایت اصلی بانک می‌شود، وارد سایت جعلی شده و اطلاعات محرمانه بانکی، اعم از شماره حساب، شماره کارت و کلمه عبور را وارد می‌نماید.

۵- روش‌های ارتقا امنیت

۵-۱- مکانیزم‌های امنیتی

مکانیزم‌های امنیتی برای مقابله با تهدیدات امنیتی در نظر گرفته شده است که بر اساس استاندارد X.800 شامل موارد زیر هستند :

۵-۱-۱- رمزنگاری

دررمزنگاری، بااستفاده از کلید خصوصی یا عمومی و با استفاده از الگوریتم‌های پیچیده ریاضی، پیام به فرمی تبدیل شود که به غیر از کاربر مجاز، کس دیگری نتواند از آن اطلاعات استفاده کند، حتی اگر به آن اطلاعات دسترسی داشته باشد. اطلاعاتی که رمزگذاری شده، تنها توسط کاربر مجازی که کلید رمز نگاری را دارد می‌تواند دوباره به فرم اولیه تبدیل شود.

۵-۱-۲- امضای دیجیتال

به زبان ساده امضای دیجیتال همان کلید خصوصی‌ای است که به فرد داده می‌شود. به کمک این امضا اگر کسی بخواهد به اطلاعات فرد دسترسی پیدا کند یا تغییراتی در آن ایجاد کند و دوباره آن را بفرستد دیگر کلید متوجه می‌شود که این اطلاعات توسط نفر سومی مشاهده یا دستکاری شده‌اند، پس آن را نمی‌پذیرد. از امضای دیجیتال می‌توان بر روی تمام بسترهای تبادل اطلاعات الکترونیک در حوزه‌های مختلف استفاده کرد. این روش، سرویس عدم انکار را برآورده می‌کند و علاوه برتحقق یکپارچگی جلوی جعل سند را نیز می‌گیرد.

۵-۱-۳- کنترل مسیریابی

استفاده از مکانیزم مسیریابی در مسیریاب‌ها برای تعیین و انتخاب مسیرها برای داده‌های ارسالی و دریافتی به یک محدوده را، کنترل مسیریابی می‌گویند. معمولاً این امکان نیز فراهم می‌شود که وقتی احتمال تهدیدات امنیتی نیز می‌رود، مسیریابی تغییر کند.

۵-۱-۴- الگوریتم Hash

یکپارچگی و صحت داده‌ها بر اساس استفاده از الگوریتم رمزنگاری خاصی با نام Hash حاصل می‌شود . در مبدا، با اجرای تابعHashروی داده، مقدار افزوده محاسبه شده و به همراه اصل داده ارسال می‌شود. در مقصد، مجدداً روی داده دریافتی، تابع Hash اعمال می‌شود. در صورت برابر بودن Hash محاسبه شده و مقدار Hash دریافتی، از عدم تغییر داده‌ها مطمئن می‌شوند.

۵-۱-۵- احراز هویت با استفاده از ویژگی‌های بیومتریک

استفاده از ویژگی‌های بیومتریک روش مناسبی برای جلوگیری از بسیاری از مشکلات امنیتی است. ویژگیهای بیومتریک مانند اثر انگشت، عنبیه، صورت، کف دست، صدا و دست خط، موارد منحصر بفردی برای هر فرد هستند که می‌توانند برای امنیت بیشتر به کار روند. همچنین می‌توان برای امنیت بیشتر از ترکیب این روش با سایر روش‌های احراز هویت استفاده کرد. برای مثال احراز هویت با اثر انگشت و اسمارت کارت.

این سیستم شامل یک اثر انگشت اسکنر و اسمارت‌کارت‌خوان است . به این تکنولوژی Match On Card می‌گویند. این سیستم، احراز هویت دارنده کارت را بدون نیاز به شبکه به‌صورت آفلاین انجام می‌دهد. این سیستم اطلاعات شخص نظیر نام و نام خانوادگی، عکس و... و اطلاعات بیومتریک را که در اینجا همان اثر انگشت کاربر است، روی Chip کارت ذخیره می‌کند. ذخیره‌سازی اثر انگشت برای هر ۱۰ انگشت دست صورت می‌گیرد که این ذخیره‌سازی به شکل عکس نیست و با استفاده از الگوریتم رمز شده اثر انگشت صورت می‌گیرد که همین امر ضامن امنیت این روش است. از مزیت‌های این روش این است که شخص نمی‌تواند هویت خود را انکار کند چون در زمان استفاده باید خود شخص به‌صورت زنده و اسمارت کارت حاوی اطلاعات بیومتریک و اطلاعات شخصی وجود داشته باشد و از دیگر مزیت‌های این دستگاه می‌توان به رمزنگاری و رمزگشایی اطلاعات اشاره کرد.

۵-۱-۶- ارتقا امنیت با حذف فیزیکی کارت

استفاده از کارت اعتباری اولین راه برای مشتریان در جهت خرید کالا و سرویس برخط است و انتقال اطلاعات کارت یک تهدید اولیه برای آنها به حساب می‌آید. در مکانیزم ارائه شده، فرایند جدیدی برای تراکنش طراحی شده است که در آن مشتری کالای مورد نظر خود را بدون استفاده از اطلاعات کارت از فروشنده خریداری می‌کند. در این فرایند مشتری پیغامی را برای خرید به بانک خود ارسال می‌کند. در عین حال ، نام بانک و نام شعبه (بدون شماره حساب) را به فروشنده ارسال می‌کند. فروشنده بدون تغییر در این اطلاعات، آنها را به در قالب درخواست به بانک خود ارسال می‌کند. بانک فروشنده درخواست را به بانک مشتری ارسال نموده و بانک مشتری این موضوع را به صورت SMS به اطلاع مشتری می‌رساند. در صورت تایید مشتری، انتقال وجه انجام شده و این موضوع به اطلاع فروشنده و مشتری رسانده می‌شود. استفاده از اطلاعات کارت به دلیل اینکه شامل اطلاعات کامل حساب می‌باشند دارای امنیت نیست که این مساله با حذف کارت در فرایند جدید حذف می‌شود. در این فرایند جدید به جای ارتباط مشتری و فروشنده، حساب‌های بانکی با یکدیگر در ارتباط خواهند بود. در این حالت فروشنده و مشتری باید دارای حساب بانکی و آدرس ایمیل معتبر باشند.

۵-۲- پروتکل های امنیتی

پروتکل‌های امن تجارت الکترونیک به عنوان یک از راه های تامین امنیت در پرداخت الکترونیک شناخته می‌شوند . هدف از طراحی این پروتکل‌ها ایجاد توانایی برای احراز هویت است که سبب ارتقاء امنیت در این نوع از تراکنش‌ها می‌شود. در این روش به دارنده کارت، فروشنده، دروازه پرداخت و صادر کننده کارت و بخش‌های مختلف اجازه داده می‌شود تا خود را به یکدیگر بشناسانند و اطلاعات را به شیوه امن و با استفاده از مکانیزم‌های امنیتی ذکر شده در بالا مثل رمز نگاری و فشرده سازی و گواهی دیجیتال رد و بدل کنند.

۵-۲-۱- پروتکل SSL

SSLرا ابتدا شرکتNetscape به منظور نقل و انتقال امن و رمزی اطلاعات ایجاد نمود و اکنون تقریبا تمام مرورگرهای استاندارد از جمله فایر فاکس، اینترنت اکسپلورر و کروم آن را پشتیبانی می‌کنند. امنیت در این پروتکل دو طرفه است؛ یعنی در هر دو طرف، فرایند رمزنگاری و رمزگشایی انجام می‌گیرد. وبسایت‌هایی که از پروتکل امنSSL جهت رمزگذاری داده‌ها استفاده می‌کنند، معمولاً از طریق پروتکل HTTPS به جای حالت عادی و غیر امن آن یعنیHTTPS با سرویس گیرنده‌ها ارتباط برقرار می‌کنند. در مرورگرها، اینگونه وبسایت‌ها معمولاً با علامت قفل سبز (به معنای ارتباط امن سالم) نشان داده می‌شوند.

در این پروتکل، همان‌طور که گفته شد، داده‌ها بین سرویس دهنده و گیرنده رمزگذاری می‌شوند؛ به همین دلیل، داده‌ها در طول انتقال از کانال غیر امن مانند اینترنت، اینترانت و ...، حفاظت شده باقی می‌مانند. هرچند دسترسی به این داده‌ها ممکن است، اما به دلیل آن‌که رمزگذاری شده اند، برای بدست آوردن داده‌های رمزگشایی شده اصلی، باید کلید مورد استفاده در آن نشست ارتباطی امن را دانست. از این رو، این پروتکل عملاً غیرقابل نفوذ است اما چون داده‌ها فقط و فقط در طول مسیر انتقال از کانال مورد نظر رمزگذاری شده اند به همین دلیل، درصورتی که بدافزاری در هر یک از این سمت‌ها قرار بگیرد، می‌تواند داده‌های اصلی را به راحتی بدزدد.

۵-۲-۲- پروتکل SET

برای غلبه بر نقاط ضعف SSL، ویزا و مستر کارت به صورت اشتراکی پروتکل SETرا توسعه دادند. پروتکل SET استاندارد پرداخت الکترونیکی براساس پول الکترونیکی می‌باشد. گذشته از تصدیق کارت اعتباری مشتری، SET شامل احراز هویت فروشنده نیز می‌باشد که در معاملات پرداخت محور مهم است.

برای استفاده از این پروتکل ، دارنده کارت اعتباری و فروشنده باید دارای گواهی باشند. این گواهی‌ها از طرف یک مرجع گواهی صادر می‌شود. در طرف خریدار، بایستی نرم‌افزار SET نصب شده و یک حساب کارت اعتباری که از SET پشتیبانی کرده و گواهی موردنیاز را فراهم می‌کند، افتتاح شود. فروشنده نیز باید نرم‌افزار را نصب کرده و آن را در ترکیب با یک نرم‌افزار مبتنی بر وب که خدمات فروش کالا را انجام می‌دهد، برای استفاده مشتریان بر روی وب قرار دهد. نرم‌افزار مورد استفاده توسط فروشنده اندکی پیچیده تر است چرا که نیاز به برقراری ارتباط با هر دو طرف خریدار و دروازه پرداخت دارد.

پروتکل SET برای تضمین نیازمندی‌هایی که اجازه محرمانه بودن اطلاعات را دارد توسعه داده شده است. این پروتکل باعث تضمین یکپارچگی تمام داده‌های منتقل شده، احراز هویت دارنده کارت و تصدیق بازرگان پذیرش کارت پرداخت می‌شود. این سیستم فاقد خواص گمنامی، عدم انکار و تحویل گواهی دار است.

۳-۲-۵- پروتکل 3DSECURE

امنیت سه طرفه یا 3DSECURE یک استاندارد فنی است که توسط ویزا کارت و مستر کارت برای تأمین امنیت بیشتر معاملات از طریق اینترنت ایجاد شده است.امنیت ۳ طرفه هنگام خرید آنلاین از کارت اعتباری خریدار در برابر استفاده غیرمجاز محافظت می‌کند. این سرویس ساده خریداران را قادر می‌سازد با درخواست کد شخصی (که معمولاً به صورت پین یکبار مصرف به تلفن همراه یا آدرس ایمیل شما ارسال می‌شود) معاملات خود را از طریق اینترنت ایمن سازند. این امر به محافظت در برابر تقلب توسط افراد غیر مجاز کمک می‌کند

هنگام فعال بودن این گزینه، چنانچه اطلاعات کارت به منظور خرید آنلاین در صفحه وبسایتی وارد شود، کاربر بصورت خودکار به صفحه دیگری منتقل می‌شود که متعلق به شرکت ارائه دهنده کارت می‌باشد. در این صفحه معمولا یا از کاربر خواسته می‌شود که رمز خود را وارد نماید و یا رمز یکبار مصرفی را که به شماره موبایل وی ارسال شده است را وارد نماید.چنانچه این رمز صحیح باشد، پرداخت تایید شده و کاربر نیز جهت ادامه فرایند خرید به سایت ارجاع دهنده بازگردانده می‌شود. به دلیل آنکه طرف ثالثی جهت تایید پرداخت، علاوه بر دارنده و پذیرنده کارت در انجام تراکنش نقش دارد، این روش "امنیت سه طرفه" نامیده شده است. مهمترین مزیت استفاده از تکنولوژی DSECURE۳ کاهش کلاهبردازی است.

۴-۲-۵- پروتکل SEPP

SEPP برای ایمن‌سازی تراکنش‌های کارت‌های بانکی برروی اینترنت توسعه یافته است SEPPبرای تراکنش‌های HTTP در نظر گرفته شده و با پرداخت‌های کارت‌های بانکی تطبیق یافته است.

شرکت هایی مانند Cyber Cash سرویسی نرم افزاری ایجاد کرده اند که اطلاعات کارت اعتباری را از روی وب سایت بازرگان دریافت می‌کند، آن را به شکل داده های POS در می‌آورد و سپس آن را به پردازشگر کارت اعتباری برای پردازش واقعی می‌فرستد. این نرم افزار را POS مجازی (Virtual pos)می‌نامند. این سیستم نیز به مشتریان خود اجازه می‌دهد تا خریدهای امن خود را با استفاده از کارت اعتباری انجام دهند. این سیستم اغلب اوقات برای خرید وفروش کالاهای فیزیکی به کار می‌رود.

۵-۲-۵- پروتکل Ecash

DigiCash به نوعی اولین نمونه از پرداخت‌های یک‌طرفه کاربران بدون دخالت بانک‌ها با استفاده از کلیدهای خصوصی رمزنگاری شده بود. راه‌اندازی سیستم کلیدهای خصوصی و عمومی رمزنگاری شده ، زمینه را برای غیرقابل ردیابی کردن پرداخت‌های الکترونیکی برای بانک‌ها و دولت‌ها فراهم کرد . این نوع سیستم امنیت را برای کاربران خود به منظور حفظ داده‌های شخصی و تامین امنیت کلیدها فراهم می‌کرد.

Ecash ادامه‌دهنده پروژه DigiCash است؛ بنا به ادعای تیم توسعه دهنده ،E-cash قادر است به سادگی ارسال یک ایمیل، پول را ارسال کند. در اصل ای کش ۳ هدف اصلی دارد:

- افزایش مقیاس پذیری(از حدود ۱۰۰ تراکنش در ثانیه به بیش از ۵ میلیون تراکنش در ثانیه)
- بهبود تجربه پرداخت که تمام تراکنش‌ها باید در عرض ۳ ثانیه به مقصد برسند.
- گسترش پروتکل و ارتقاء شبکه بدون نیاز به فورک.

این پروتکل سطح بالایی از گمنامی را فراهم کرده است ولی خواص اتمی را در هیچ نوع آن دارا نمی‌باشد.

۶-۲-۵- پروتکل NetBill

در این سیستم با استفاده از رمز کردن پیام‌های ارسالی و همچنین امضا کردن مبلغ کالا و سایر پارامتر های توافقی خواص اتمی به خوبی اقناع شده اند ولی مشکل این سیستم برخورداری از اعمال رمز نگاری فراوان و ارسال پیام‌های زائد بسیار است که از کارایی این سیستم تا حدی کاسته است .

۷-۲-۵- پروتکل Milicent

در این سیستم همواره سه رابطه بین کلید خصوصی فروشنده ، شناسه خریدار و کلید خصوصی خریدار وجود دارد که فروشنده به راحتی می‌تواند درستی یا نادرستی آن را تایید کند ولی به این ترتیب خاصیت گمنامی به هیچ وجه اقناع نمی‌شود و علاوه بر آن خواص اتمی نیز در هیچ شکلی در این سیستم لحاظ نشده است .

۶- نتیجه‌گیری

تجارت الکترونیکی یک جزء اصلی عملیات کسب و کار شده است و بر پایه پرداخت الکترونیکی ساخته شده است. در مقایسه با روش‌های پرداخت سنتی، روش‌های پرداخت الکترونیکی مزیت‌هایی دارد که شامل امنیت، قابلیت اعتماد، گمنامی، مقبولیت، محرمانگی، کارآیی و راحتی می‌باشد. . مهمترین نگرانی در پرداخت‌های الکترونیکی ، سطح امنیت در هر مرحله از تراکنش است زیرا کالا و پول در حالی انتقال می‌یابد که هیچ ارتباط مستقیمی بین دو طرف تراکنش وجود ندارد. در این مقاله ، یک بررسی از دسته‌بندی‌های مختلف تهدیدات امنیتی و روش‌های ارتقا امنیت پرداخت الکترونیکی انجام گرفت. در حوزه مکانیزم‌های راهی ارائه گردید که در آن از ترکیب ویژگی بیومتریک مانند اثرانگشت برای افزیش امنیت پرداخت استفاده شود. در بخش امنیت کارت نیز با ارایه راهکار، سعی در حذف کارت به صورت فیزیکی شده است که تاثیر بسزایی در ارتقاء امنیت در پرداخت می‌نماید. در نهایت پروتکل‌های پرداخت الکترونیکی امن همانند، 3DSECURE، SET، ، SSLو... بررسی شد. این راهکارهای امنیتی بستر رمزنگاری را برای انجام تراکنش‌های برخط فراهم می‌کنند که سبب عدم امکان خواندن اطلاعات در زمان انتقال می‌شوند.

با این حال امروزه مشخص شده است که این راهکارها نیز دارای نقاط ضعفی هستند و آنگونه که تاکنون تصور می‌شده است امنیت ما را تامین نمی‌کنند. با این حال و در شرایط جاری که با گسترش تکنولوژی‌ها و توسعه

نرم افزارها روبه رو هستیم، این رویکرد نیز باید تغییر یافته و شکل دیگری به خود بگیرد. همچنین اکثریت سیستم‌های مطرح شده قابل توسعه بوده و با در نظر گرفتن بستر مناسب، سیاست‌های حاکم، امکانات در دسترس، موجودیت-های معتبر و شرایط مد نظر، قابل انتخاب و استفاده و بهره‌برداری‌اند.

مراجع

[۱] همرام ، جواد ، **بررسی امنیتی سیستم‌های پرداخت الکترونیکی آنلاین**، دومین همایش ملی پژوهش های کاربردی در علوم کامپیوتر و فناوری اطلاعات ،۱۳۹۳ .

[۲] سلماسی_زاده ، محمود و سهی_زاده، محمدرضا **روش_های پرداخت الکترونیک و امنیت آنها** ، سومین همایش ملی تجارت الکترونیک ، ۱۳۸۴.

[۳] صیامی ، وحید ، **پرداخت الکترونیک به زبان ساده**، چاپ اول، انتشارات راه‌دان، ۱۳۹۳.

[۴] فکور ثقیه، امیر محمد، **بانکداری الکترونیک، از تئوری تا عمل**، ، چاپ اول، نشر ترانه ، ۱۳۸۸.

[۵] کاظمی‌راد،محمدکاظم، **پرداخت الکترونیک: مقدمه‌ای بر صنعت پرداخت ایران**، تهران، انتشارات راه پرداخت ، ۱۳۹۹.

[۶] مختاری ، ابراهیم و صوفیوند ، فاطمه ، **بررسی انواع روش‌های پرداخت الکترونیک و امنیت آنها**، کنفرانس بین المللی حسابداری و مدیریت ، ۱۳۹۳.

[۷] معینی، علی و حسن‌زاده، پروین،**سیستم‌های پرداخت الکترونیکی**، انتشارات ادیبان روز،۱۳۹۵.

[8] Jerrin Y, Chitra K, *A Critical Analysis on the Evolution in the E-Payment ystem, Secuiry Risk, Threats and Vulnerability* , Pacific Press, London,2018.

[9] Naeem M, Hameed M, Sabah Taha M, *A study of electronic payment system*, School of Computing, UUM, College of Arts and Science, 2021.

[10] Aigbe P, Akpojaro J, *Analysis of Security Issues in Electronic Payment Systems*, International Journal of Computer Applications, 2014.

[11] Solat S,*Security of Electronic Payment Systems: A Comprehensive Survey* , Sorbonne Universités, UPMC University of Paris VI, French National Centre for Scientific Research CNRS, Computer Laboratory,2017.

[12] https://fa.wikipedia.org/wiki/امنیت اطلاعات

[13] https://en.wikipedia.org/Smart card acts as a secure electronic payment system