

صلى الله عليه وسلم



دانشکده آموزش های الکترونیکی

پایان نامه کارشناسی ارشد در رشته مهندسی فناوری اطلاعات
(تجارت الکترونیک)

بررسی امنیت وب سرویس در معماری سرویس گرا و ارائه یک مدل امنیتی
برای وب سرویس پرداخت الکترونیکی

به کوشش:

رضا محمدپور دوانی کبیر

استاد محترم راهنما:

دکتر محمد هادی صدرالدینی

مرداد ۱۳۹۱

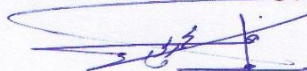
بسمه تعالی

اظہارنامہ

اینجانب رضا محمد پور دوانی کبیر(۸۸۸۴۶۷) دانشجوی رشته مهندسی IT
گرایش تجارت الکترونیک دانشکده آموزش های الکترونیک دانشگاه شیراز اظهار
می کنم که این پایان نامه حاصل پژوهش خودم بوده و در جاهایی که از
منابع دیگران استفاده کرده ام، نشانی دقیق و مشخصات کامل آن را
نوشته ام. همچنین اظهار می کنم که تحقیق و موضوع پایان نامه ام
تکراری نیست و تعهد می نمایم که بدون مجوز دانشگاه دستاوردهای
آن را منتشر ننموده و یا در اختیار غیر قرار ندهم. کلیه حقوق این اثر
مطابق با آیین نامه مالکیت فکری و معنوی متعلق به دانشکده آموزش
های الکترونیکی دانشگاه شیراز می باشد.

نام و نام خانوادگی : رضا محمدپور دوانی کبیر

امضا و تاریخ :



۹۱/۵/۱۰

به نام خدا

بررسی امنیت وب سرویس در معماری سرویس گرا و ارائه یک مدل امنیتی

برای وب سرویس پرداخت الکترونیکی

به کوشش

رضا محمدپوردوانی کبیر

پایان نامه

ارائه شده به تحصیلات تکمیلی دانشگاه شیراز به عنوان بخشی

از فعالیت های تحصیلی لازم برای اخذ درجه کارشناسی ارشد

در رشته ی:

مهندسی فناوری اطلاعات (گرایش تجارت الکترونیک)

از دانشگاه شیراز

شیراز

جمهوری اسلامی ایران

ارزیابی کمیته پایان نامه، با درجه ی: عالی.....

دکتر محمد هادی صدرالدینی، دانشیار بخش مهندسی و علوم کامپیوتر و فناوری اطلاعات (رئیس کمیته)

دکتر علی حمزه، استادیار بخش مهندسی و علوم کامپیوتر و فناوری اطلاعات

دکتر رضا اکبری، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، استادیار دانشگاه صنعتی شیراز

مرداد ۱۳۹۱

تقدیم بہ آنان کہ شادیشان آرزوی من است

پدر و مادر مہربانم

ہمسر صمیمی و عزیزم

دختر و بلندم

تشکر و قدردانی

شکر و سپاس از ایزد یکتا و هستی بخش که الطافش را بر من همواره جاری فرمود و مرا تا رسیدن به این نقطه یاری کرد. با سپاس و قدردانی فراوان، از استاد گرامی و دلسوزم جناب آقای دکتر صدرالدینی که با راهنمایی ها و نظرات ارزشمندشان به من یاری رساندند و مرا در سختی های این مسیر پشتیبانی نمودند. همچنین تشکر و احترام فراوان خدمت اساتید مشاور محترم جناب دکتر حمزه و جناب دکتر اکبری، اساتید گرامی مشاورم که قبول زحمت فرمودند و راهنمایی های ارزشمندشان روشنگر راهم بود. از تمامی اساتید، پرسنل، دوستان و تمام کسانی که در دانشگاه، آن محیط کسب دانش و معرفت، فضایی خاطره انگیز را به وجود آوردند، کمال تشکر را دارم

چکیده

بررسی امنیت وب سرویس در معماری سرویس گرا و ارائه یک مدل امنیتی برای وب سرویس پرداخت الکترونیکی

به کوشش

رضا محمدپور دوانی کبیر

امروزه بهره‌گیری از وب سرویس‌ها به عنوان راهکاری جدی جهت یکپارچه سازی تعامل‌ها در سطح بنگاه‌های مختلف مطرح است، بهره‌گیری از سیستم مذکور بدون در نظر گرفتن نکات امنیتی در وب سرویس‌ها کاری بیهوده است. بدلیل اهمیت بالای سرویس‌های پرداخت الکترونیکی، تکنیک‌های زیادی جهت ایجاد امنیت کاربران و بانک‌ها برای خرید و فروش امن در شبکه‌های اینترنتی مطرح شده است که هر یک بر اساس ایده‌ای خاص سعی در برقراری امنیت در فعالیت‌های خرید و فروش دارند. هدف از پایان‌نامه مطالعه فنی مهم‌ترین تکنیک‌های امنیتی در وب سرویس‌های اینترنتی و پرداخت الکترونیکی می‌باشد. سپس بر اساس مطالعه مهم‌ترین روش‌های امنیتی، مدل امنیتی جدیدی جهت بالا بردن ضریب امنیتی وب سرویس‌های پرداخت الکترونیکی ارائه شده است. در انتهای پایان‌نامه، این مدل جدید با سایر مدل‌ها مقایسه گردیده و نقاط قوت و ضعف آن بیان شده است.

کلمات کلیدی : وب سرویس - معماری سرویس گرا - رمزنگاری متقارن - رمزنگاری نا

متقارن - کلید عمومی - کلید خصوصی

فهرست مطالب

عنوان صفحه

فصل اول: مقدمه و طرح مساله

۱-۱ مقدمه..... ۲

۲-۱ ضرورت و اهمیت موضوع..... ۳

۳-۱ بیان مسئله ۵

۴-۱ دامنه تحقیق..... ۶

۴-۱-۱ پروتکل دسترسی ساده به شیء (SOAP)..... ۶

۴-۱-۲ زبان توصیف خدمات وب (WSDL)..... ۷

۴-۱-۳ شرح، کشف و یکپارچه‌سازی جهانی (WSDL)..... ۷

۵-۱ هدف تحقیق ۷

فصل دوم: مبانی نظریه

۱-۲ مقدمه ۱۰

۲-۲-۱ انواع سبک های استفاده از وب سرویس ها..... ۱۰

۲-۲-۱-۱ روش فراخوانی از راه دور RPC..... ۱۰

۲-۲-۲ معماری سرویس‌گرا ۱۱

۱۲ نمایانگر حالت انتقال (REST) (REST)
۱۲ WS-I Basic Profile و مشخصه های امنیتی سرویس های وب
۱۵ مشخصه های وب سرویس
۱۵ امنیت وب سرویس ها
۱۶ سیاستگذاری سرویس وب
۱۶ آدرس دهی سرویس وب
۱۶ پیغام رسانی سرویس وب
۱۷ مکالمه ایمن سرویس وب
۱۷ پیغام رسانی مطمئن سرویس وب
۱۸ معایب
۱۸ WS SECURITY فواید
۱۹ امضای XML چیست
۲۰ مشخصات امضای دیجیتال
۲۱ تاریخچه شکل گیری طرح امضای دیجیتال
۲۳ معایب امضای دیجیتال
۲۵ مزایای XML Signature
۲۶ رمزنگاری در ساختار امضای XML
۲۷ انواع رمزنگاری :

- ۳۳-۲-۷-۲ - مقایسه الگوریتم‌های رمزنگاری متقارن و کلید عمومی ۳۳
- ۳۳-۳-۷-۲ - تولید کد ۳۳
- ۳۳-۴-۷-۲ - پروتکل رمزنگاری ۳۳

فصل سوم: مروری بر تحقیقات انجام شده

- ۳۷-۱-۳ - مقدمه ۳۷
- ۳۷-۱-۲-۳ - پرداخت‌های الکترونیکی ۳۷
- ۴۴-۲-۲-۳ - سیستم‌های بانکی الکترونیک ۴۴
- ۴۸-۳-۲-۳ - وظایف بانک مرکزی در اعمال اصول بنیادین ۴۸
- ۴۹-۳-۳ - بررسی سایر روش‌های امنیتی در پرداخت الکترونیک ۴۹
- ۴۹-۱-۳-۳ - سیستم‌های پرداخت الکترونیک با استفاده از روش رمزنگاری ۴۹
- ۴۹-۲-۳-۳ - مدل احراز هویت Kerberos ۴۹
- ۵۰-۳-۳-۳ - مقایسه مدل‌های Micro_payment با مدل‌های جاری Macro_payment ۵۰
- ۵۰-۴-۳-۳ - ارائه مدل کنترل دسترسی مبتنی بر وکالت در معماری سرویس‌گرا ۵۰
- ۵۱-۵-۳-۳ - سرویس‌های REST (State Transfer Representational) ۵۱

فصل چهارم: ارائه راهکار، الگوریتم و طرح پیشنهادی

- ۵۴-۱-۴ - مقدمه ۵۴
- ۵۴-۲-۴ - طرح پیشنهادی ۵۴
- ۵۵-۳-۴ - مطالعه فنی طرح جدید ۵۵

فصل پنجم: نتیجه گیری و پیشنهادها

۶۰	۱-۵ - مقدمه
۶۰	۲-۵ - مقایسه مدل امنیتی ارائه شده و مدل های موجود
۶۱	۳-۵ - ارزیابی فنی طرح پیشنهادی با مدل استاندارد WS-SECURITY
۶۵	۴-۵ - مزایای طرح پیشنهادی
۶۵	۵-۵ - معایب طرح پیشنهادی
۶۵	۶-۵ - نتیجه گیری
۶۶	۷-۵ - کارهای آینده
۷۹	فهرست منابع
۶۷	پیوست ها

فهرست تصاویر

عنوان	صفحه
شکل ۵-۱ مقایسه مدل پیشنهادی با مدل استاندارد.....	۶۱
شکل ۵-۲ خروجی نرم افزار مقایسه کننده.....	۶۲
شکل ۵-۳ کد واسط روپس پرداخت.....	۶۶
شکل ۵-۴ کد کلاس سرویس.....	۶۷
شکل ۵-۵ ایجاد کلید های موقتی خصوصی و عمومی ۱.....	۶۹
شکل ۵-۶ ایجاد کلید های موقتی خصوصی و عمومی ۲.....	۶۹
شکل ۵-۷ کد احراز هویت کاربران	۷۰
شکل ۵-۸ کد مدیریت لایه بانک اطلاعات	۷۱
شکل ۵-۹ کد احراز هویت کاربر	۷۲
شکل ۵-۱۰ کد وب سایت جهت استفاده از وب سرویس و انجام عملیات بانکی.....	۷۳
شکل ۵-۱۱ فایل تنظیمات وب سرویس	۷۴
شکل ۵-۱۲ ادامه فایل تنظیمات وب سرویس.....	۷۵
شکل ۵-۱۳ فایل تنظیمات وب سایت سرویس گیرنده.....	۷۶
شکل ۵-۱۴ ادامه فایل تنظیمات وب سایت سرویس گیرنده.....	۷۷

فصل اول

مقدمه و طرح مسئله

۱-۱ مقدمه

معماری سرویس گرا امکان توزیع برنامه های کاربردی را در شبکه و اینترنت فراهم می سازد. یعنی می توان برنامه های کاربردی و تحت وب را بصورت سرویس های توزیع شده در کامپیوتر های مختلف، بصورت یکپارچه و یا از راه دور اجرا نمود. به سرویس های استفاده شده در معماری سرویس گرا، وب سرویس^۱ گفته می شود. وب سرویس نرم افزاری است که دسترسی به اطلاعات و سیستم های پردازش اطلاعات را بصورت توزیع شده^۲، بدون وابستگی به محیط^۳ سخت افزاری و نرم افزاری خاصی، با استفاده از قوانین استاندارد امکان پذیر می کند. امروزه از وب سرویس ها به عنوان راهکاری در راستای یکپارچه سازی تعامل ها در سطح بنگاه ها از جمله بنگاه های اقتصادی، استفاده می گردد. وب سرویس هایی که در بنگاه های اقتصادی وظیفه پرداخت، دریافت و عملیات مالی را بر عهده دارند، وب سرویس های پرداخت الکترونیکی گفته می شوند. بهره گیری از سیستم مذکور بدون در نظر گرفتن نکات امنیتی در وب سرویس ها کاری بیهوده می باشد. بدون شک سرویس وب یکی از مهمترین سرویس های موجود بر روی اینترنت است که بیشترین تاثیر را در عمومیت یافتن اینترنت در سطح جوامع بشری برعهده داشته است. وب در نگاه اول مانند یک سیستم اطلاعاتی توزیع شده است. در سیستم فوق اطلاعات (با اشکال متفاوت) بر اساس استانداردهای مربوطه و با یک ساختار مشخص قرار گرفته و با استفاده از ارتباطات تعریف شده بین اطلاعات می توان به سرعت و به سادگی از اطلاعات موجود استفاده کرد. در این پایان نامه ضمن معرفی وب سرویس ها به تعریف مبانی امنیت در حوزه وب و نحوه انطباق آن با اصول وب سرویس ها جهت ارائه راهکارهای امن در

¹ Web Service

² Distributed

³ Platform

پیاده سازی وب سرویس‌ها می‌پردازیم. به دلیل اهمیت بالای وب سرویس‌های پرداخت الکترونیکی، تکنیک‌های زیادی جهت ایجاد امنیت کاربران و بانک‌ها برای خرید و فروش امن در شبکه‌های اینترنتی مطرح شده است که هر یک بر اساس ایده‌ای خاص سعی در برقراری امنیت در بخشی یا تمامی فعالیت‌های خرید و فروش دارند. هدف از پایان‌نامه مطالعه فنی مهمترین تکنیک‌های امنیتی در سرویس‌های اینترنتی و پرداخت الکترونیکی می‌باشد. سپس بر اساس مطالعه مهمترین روش‌های امنیتی، مدل امنیتی جدیدی جهت بالا بردن ضریب امنیتی وب سرویس‌های پرداخت الکترونیکی ارائه شده است. در انتهای پایان‌نامه، این مدل جدید با سایر مدل‌ها مقایسه گردیده و نقاط قوت و ضعف آن بیان شده است.

۱-۲ ضرورت و اهمیت موضوع

اهمیت موضوع این پایان‌نامه از دو جنبه بررسی می‌گردد:

۱- بررسی امنیت وب سرویس در معماری سرویس‌گرا

وب سرویس یکی از اجزاء مهم در پیاده سازی معماری سرویس‌گرا می‌باشد، زیرا می‌توان وب سرویس‌ها را مستقل از نوع سخت افزار و سیستم عامل از هر نقطه فراخوانی نموده و از سرویس درونی آن استفاده کرد. از مهمترین وظایف وب سرویس‌ها مدیریت اطلاعات می‌باشد. دولت‌ها، مراکز نظامی، شرکت‌ها، موسسات مالی، بیمارستان‌ها و مشاغل خصوصی مقدار زیادی اطلاعات محرمانه در مورد کارکنان، مشتریان، محصولات، تحقیقات و وضعیت مالی گردآوری می‌کنند. بسیاری از این اطلاعات در حال حاضر بر روی کامپیوترهای الکترونیکی جمع‌آوری، پردازش و ذخیره شده و از طریق شبکه به کامپیوترهای دیگر منتقل می‌شوند. اگر اطلاعات محرمانه در مورد مشتریان، امور مالی یا محصول جدید به دست رقیب بیفتند، ممکن است به خسارات مالی در کسب و کار، پیگرد قانونی و یا حتی ورشکستگی منجر شوند. بنابراین اگر وب سرویس‌هایی که مدیریت اطلاعات را بر عهده دارند، نتوانند امنیت کافی را در شبکه‌ها و اینترنت برقرار نمایند خسارت‌های جبران

ناپذیری ایجاد می کنند. از اینرو تکنیک های مهم و استانداردی جهت برقراری امنیت در وب سرویس ها ارائه شده اند که در این پایان نامه به مطالعه آنها می پردازیم.

۲- مدل امنیتی برای وب سرویس پرداخت الکترونیکی

امروزه خدمات بانکی یکی از مهمترین سرویس های تحت وب می باشند. تعداد مشترکین خدمات بانکداری با رشد چشمگیری در سالهای اخیر مواجه بوده اند. ارائه سرویس های بانکی در اینترنت، موبایل و شبکه های خصوصی بانک ها توسط وب سرویس های پرداخت الکترونیکی انجام می شوند. امنیت مهمترین اصل در پیاده وب سرویس های پرداخت الکترونیکی می باشد، زیرا در وب سرویس ها عملیات بانکی از راه دور و خارج از سازمان اقتصادی مربوطه انجام می پذیرند. بحث امنیت در سال های اخیر به میزان قابل توجهی رشد کرده است و تکامل یافته است. راه های بسیاری برای ورود به این حوزه کاری به عنوان یک حرفه وجود دارد. موضوعات تخصصی در زمینه امنیت را می توان، تامین امنیت شبکه، تامین امنیت برنامه های کاربردی، پایگاه داده ها، تست امنیت، حسابرسی و بررسی سیستم های اطلاعاتی، بررسی جرائم الکترونیکی و غیره برشمرد [۲۹ و ۳۰]. بنابراین بدون وجود الگوهای امنیتی در پیاده سازی سرویس های بانکی، امکان دزدی و کلاهبرداری افزایش می یابد.

نیاز به ارائه مدل های امنیتی جدید، جهت جلوگیری از حملات کلاهبرداران اقتصادی بسیار حائز اهمیت می باشد. در این پایان نامه یک الگوی امنیتی جدید جهت افزایش امنیت پرداخت الکترونیکی ارائه شده است.

3-1 بیان مسئله

معماری سرویس‌گرا تعاملات مختلف تحت وب را یکپارچه نموده و هر تعامل را بصورت یک وب سرویس پیاده‌سازی می‌کند، از این‌رو به عنوان یکی از روش‌های مهم برای ساخت سیستم‌های توزیع شده استفاده می‌گردد. همچنین می‌تواند کارکردهای نرم‌افزاری را در قالب سرویس‌ها ارائه کند. این معماری جهت یکپارچه‌سازی ارتباطات در یک یا چند سازمان، از طریق وب یا شبکه‌های محلی و خصوصی استفاده می‌گردد. سرویس‌گیرندگان مانند برنامه‌های کاربردی یا کاربران، می‌توانند با استفاده از معماری سرویس‌گرا، وب سرویس‌ها را از راه دور فراخوانی کنند و نتیجه پردازش را از طریق وب یا شبکه محلی دریافت نمایند. وب سرویس نرم‌افزاری است که امکان دسترسی به اطلاعات و عملیات پردازش اطلاعات را بصورت توزیع شده و مستقل از نوع سخت‌افزار، سیستم عامل و سرویس‌دهندگان فراهم می‌سازد. وب سرویس با پشتیبانی از تمام قوانین استاندارد، تعامل عملیاتی و انتقال اطلاعات را بین شرکت‌ها، بانک‌ها، کاربران و بنگاه‌های تجاری و اقتصادی فراهم می‌سازد. امنیت از مهمترین مقوله‌ها در فناوری اطلاعات می‌باشد. بسیاری از سرویس‌ها بایستی فقط توسط افراد سازمان یا مشتریان آن سرویس مورد استفاده قرار گیرند. معماری سرویس‌گرا از طریق تکنیک‌های مختلف امنیتی و احراز هویت می‌تواند دسترسی افراد ناشناس و غیر معتبر را از وب سرویس‌ها سلب نماید. تولیدکنندگان وب سرویس‌ها، در هنگام استفاده از وب سرویس‌ها در شبکه‌های غیر امن مانند اینترنت، باید یک الگوی امنیتی در وب سرویس‌های خود پیاده‌سازی کنند تا از دزدی اطلاعات جلوگیری نمایند [۱۰ و ۷]. در این پایان‌نامه مهمترین استانداردها و الگوهای امنیتی از نظر فنی بررسی و مقایسه شده‌اند و یک الگوی جدید امنیتی بر اساس استانداردهای موجود ارائه گردیده‌است.

۴-۱ دامنه تحقیق

از زمان مطرح شدن مفهوم شبکه و وب، طرح های زیادی برای امنیت در وب سرویس ها ارائه گردیده است که منجر به شکل گیری استانداردهای مهمی شده است که در ادامه به آنها می پردازیم. به دلیل اهمیت بالای سرویس های پرداخت الکترونیکی، روش های زیادی جهت ایجاد امنیت کاربران و بانک ها برای خرید و فروش امن در شبکه های اینترنتی مطرح شده است که هر یک بر اساس ایده های خاص، سعی در برقراری امنیت در فعالیت های خرید و فروش دارند. به دلیل گستردگی تکنیک های امنیتی در وب سرویس ها، روش هایی که امروزه به عنوان مهمترین روش ها در اینترنت و سیستم های پرداخت استفاده می شوند، به عنوان دامنه تحقیق انتخاب گردیده اند. دامنه تحقیق بررسی فنی و شناخت حرفه ای از پروتکل های SOAP، XML Encryption، XML Signature، WS-Security و تکنیک رمز نگاری های X.509 و Kerberos می باشد [۲۹۱].

۴-۱-۱ پروتکل دسترسی ساده به شیء (SOAP)

بر اساس پروتکل دستیابی ساده به شیء، تمامی خدمات وب به گردش در می آیند. منظور از پروتکل، مجموعه شرح قواعد و فرمت های مربوط به ارسال پیام های مخابراتی از یک ماشین به ماشین دیگر است. SOAP پروتکل ساده ای است که به منظور سازگاری^۱ با سکوهای^۲ مختلف و نیز سیستم های عامل^۳ گوناگون ایجاد شده است. هدف اصلی این پروتکل، امکان پذیری ارسال اطلاعات از ماشین به ماشین دیگری در محیط های محاسباتی نامتجانس^۴ می باشد [۲۸ و ۲۹].

¹ Compatibility

² Platforms

³ Operating systems

⁴ Heterogeneous

۱-۴-۲ زبان توصیف خدمات وب (WSDL)

هر چه بیشتر پروتکل‌های مخابراتی و فرمت پیام‌ها بر روی وب به سمت استاندارد شدن پیش می‌روند، امکان توصیف تبادلات، به شیوه‌های ساختارپذیر^۱ نیز افزایش می‌یابد. زبان توصیف خدمات وب، به منظور برآورده نمودن همین نیاز ابداع گردیده‌است، و این هدف را با تعریف یک گرامر از نوع XML انجام می‌دهد. این گرامر خاص، عملیات موجود در شبکه را به صورت مجموعه‌هایی از اطلاعات نهایی قابل ارسال پیاده‌سازی می‌کند. بنابراین توسط این اطلاعات، می‌توان پیام‌های مورد نیاز را در شبکه ارسال و دریافت نمود [۲۸ و ۲۹].

۱-۴-۳ شرح، کشف و یکپارچه‌سازی جهانی (UDDI)

به وسیله فناوری شرح، کشف و یکپارچه‌سازی فراگیر^۲ می‌توان به انتشار و جستجوی خدمات وب پرداخت. این فناوری، خدمات وب را سامان داده و پس از شرح خدمات مورد نیاز، اطلاعات بدست آمده را در یک جایگاه مرکزی بصورت یکپارچه ذخیره نماید. در این روش به جای استفاده از پیام‌ها و عملیات، تاکید بر تعامل با منابعی است که حالت پذیر^۳ هستند [۲۸ و ۲۹].

۱-۵ هدف تحقیق

در ابتدا، تجارت الکترونیک، روشی بیش از یک اطلاع رسانی ساده نبود و هرکس می‌توانست محصولات خود را با استفاده از صفحات وب بر روی اینترنت تبلیغ نماید. اما اکنون هدف از به کارگیری تجارت الکترونیک، ارائه روشی جدید در انجام امور بازرگانی می‌باشد. تجارت الکترونیکی ترکیبی از روش‌ها و شگردهای بازرگانی است که می‌توانند همکاری، رقابت و

¹ Structured

² Universal Description, Discovery and Integration

³ State full

بازدهی بیشتری برای شرکت‌ها ایجاد نمایند. از اینرو تجارت الکترونیکی طی ۱۵ سال گذشته سبب شده است که شرکت‌ها روش‌های تجارتي خود را اصلاح نموده و در زمینه‌های ارتباطی با شرکت‌های دیگر، پیشرفت‌های مهمی ایجاد نمایند. همچنین گسترش دامنه بازرگانی و تجاری حتی در مقیاس‌های بزرگ و جهانی از مزایای تجارت الکترونیک بوده است. هدف از تحقیق، مطالعه فنی مهم‌ترین روش‌های امنیتی در سرویس‌های اینترنتی و پرداخت الکترونیکی می‌باشد. در انتهای پایان‌نامه، بر اساس مطالعه مهم‌ترین روش‌های امنیتی، الگوی جدیدی جهت بالا بردن ضریب امنیتی وب سرویس‌های پرداخت الکترونیکی ارائه شده است.