



انتشارات ادیان روز

سیستم‌های پردازش الکترونیکی

دکتر علی معینی
(عضو هیات علمی دانشگاه تهران)
مهندس پروین حسن‌زاده

سرشناسه :	معینی، علی، ۱۳۳۷ -
عنوان و نام پدیدآور :	سیستم‌های پرداخت الکترونیکی / علی معینی، پروین حسن‌زاده.
مشخصات نشر :	تهران: ادیبان روز، ۱۳۹۵
مشخصات ظاهری :	۱۹۲ ص.
شابک :	۹۷۸-۶۰۰-۸۱۹۰-۴۵-۵
وضعیت فهرست نویسی :	فیبا
موضوع :	انتقال الکترونیکی وجوه
موضوع :	Electronic funds transfers
موضوع :	بازرگانی الکترونیکی
موضوع :	Electronic commerce
موضوع :	بازرگانی الکترونیکی -- تدابیر ایمنی
موضوع :	Electronic commerce -- Security measures
شماره افزوده :	حسن‌زاده، پروین، ۱۳۶۸ -
رده بندی کتبی :	۱۳۹۵ س ۹ / م ۶ / ۱۷۱۰ HG
رده بندی دیوید :	۳۳۲ / ۱۷۸
شماره کتابخانه ملی :	۴۵۲۷۰۴۹

مؤلفین :	علی معینی - پروین حسن‌زاده
گرافیک و صفحه آرا :	مریم علی‌زاده
طراح جلد :	فانیه بهروز صفا
شمارگان :	۱۰۰۰
قیمت :	۱۵۰۰۰ تومان
شابک :	۹۷۸-۶۰۰-۸۱۹۰-۴۵-۵
تاریخ انتشار :	زمستان ۹۵
نویت چاپ :	اول
چاپ و صحافی :	طوس

کلیه حقوق این اثر متعلق به انتشارات ادیبان روز می‌باشد و هرگونه استفاده از این کتاب (کپی تکریر، استفاده در کارگاه‌های آموزشی) بدون اجازه ناشر پیگرد قانونی دارد.

تلفن : ۶۶۹۵۶۸۱۲-۱۵

خرید اینترنتی از طریق:

www.adibanbook.com

www.adibanbook.ir



انتشارات ادیبان روز

پیش گفتار

این کتاب به تکنیک‌ها و سیستم‌های پرداخت به کمک اینترنت می‌پردازد، که در درجه اول می‌تواند به عنوان کتاب درسی ۳ واحدی برای مقطع کارشناسی یا کارشناسی ارشد ارائه گردد. در صورت ۱ واحدی بودن درس، می‌توان سه فصل ششم، هفتم و هشتم را حذف نمود. همچنین این کتاب می‌تواند در نگاه جامعی از بهترین روش‌های پرداخت الکترونیک را برای محققان و متخصصان صنعت بیم که نیازمند درک گسترده‌ای از فناوری‌های مهم در این حوزه هستند، ارائه نماید. فصل اول این پژوهش، نارسندیه‌های سامانه‌های پرداخت و ویژگی‌های تراکنش‌ها را ارائه می‌دهد. فصل دوم ارائه‌دهنده‌ی بحث در زمینه‌ی روش‌های پرداخت نقدی، پرداخت از طریق بانک، پرداخت با چک، پرداخت با جایز، پرداخت‌های اتاق تسویه اتوماتیک، پرداخت با کارت اعتباری می‌باشد. در ادامه‌ی این فصل جا، حساب بانکی و تنظیم مقررات معرفی می‌گردد. در فصل سوم که دانش خوبی را در حیطه‌ی امنیت، ارائه می‌نماید، رمزگذاری متقارن داده و رمزگذاری نامتقارن، استاندارد رمزگذاری داده، استاندارد رمزگذاری پیشرفته، الگوریتم‌های درهم‌سازی، امضای دیجیتال و امضای دوتایی از جمله مباحث هستند که به آن‌ها پرداخته‌شده است. فصل چهارم انواع کارت‌ها و میزان حافظه آن‌ها، مراحل پرداخت با کارت اعتباری به کمک پروتکل سوکت امن و نحوه استفاده از کارت بدهی را ارائه خواهد کرد. فصل پنجم به مبحث چک‌های الکترونیکی و انتقال بین حساب‌ها می‌پردازد. علاوه بر این FSML، Swift و از جمله مباحثی است که این فصل به آن پرداخته است. فصل ششم پرداخت نقدی الکترونیکی و سکه‌های Ecash را ارائه خواهد کرد و جهت تکمیل این مباحث راهکارهایی جهت جلوگیری از تقلب، هزینه مجدد و یافتن سکه‌های گم‌شده را مورد بررسی قرار خواهد داد. به دلیل اینکه در بعضی از پرداخت‌ها، باید مبلغ ناچیزی پرداخت شود در فصل هفتم به این سامانه‌های پرداخت خرد پرداخته‌شده است. با گسترش روزافزون تلفن همراه، لزوم

مفهوم تجارت سیار معنا پیدا می‌کند که به این مبحث و کنفرسیوم‌های EC، اپراتورهای شبکه موبایل و سامانه‌های پرداخت بر اساس کارت اعتباری در شبکه‌های تلفن همراه در فصل هشتم پرداخته شده است.

بدون تردید این کتاب خالی از اشکال نیست که ضمن پوزش از شما خواننده محترم استدعا داریم هر گونه نقد و پیشنهاد خود را به آدرس الکترونیکی Hassanzadeh.ec@gmail.com ارسال فرمایید تا در ریز این بعدی اصلاح شود.

علی معینی

پروین حسن‌زاده

تابستان ۹۵

در هر اقتصاد مدرنی که بر مبنای مبادلات تجاری توسعه یافته است، با روش های پرداخت پول سروکار دارد. مواقع پرداخت نشان دهنده انتقال پول از ذینفع به فروشنده یک کالا یا خدمات می باشد. روش های پرداخت را می توان در سیستم های قدیمی دادوستد کالا که نمایانگر نوعی از پرداخت از طریق تبادل، تنقسم کالا است، جستجو کرد. با توجه به انعطاف پذیری پایین این روش، سامانه های پرداخت مبتنی بر پول اعتباری و بسیاری از سیستم های پیشرفته توسعه یافته اند. در طول دوره معاصر، یک سیستم پرداخت، نشان دهنده ی مجموعه ای از فرآیندها و شبکه های کامپیوتری است که برای ایجاد تراکنش های مالی بر روی ارزش های ارائه شده توسط بازار، و بازار پول استفاده می شود. مسئله دیگر این است که پرداخت ها توسط مشتریان خرده فروشی بر روی ارزش های ارائه شده توسط بازار و پول استفاده می شود.

در جهان امروز، شکل مرسوم از مظاهر پرداخت شامل پول، چک ها، حواله های بانکی و در مورد فرآیندهای کسب و کار از قبیل پرداخت، معمولا از طریق یک فاکتور یا یک رسید، انجام می شود. در حال حاضر، صنعت پرداخت الکترونیک بر مبنای نقل و انتقالات الکترونیکی مبتنی بر کارت متمرکز شده است و پیاده سازی های موفق بسیاری نیز وجود دارد. همه ی این دستگاه ها بر روی کارت یا حساب بانکی متمرکز شده اند و این بدان معناست که کاربر باید برای انتقال پول با بانک ارتباط برقرار کند.

سیستم های پرداخت الکترونیک، به عنوان بخش مهمی از تجارت الکترونیک و کسب و کار الکترونیک بوده و توسعه آن ها مهم می باشد. به هر حال، روش های سنتی پرداخت برای کالا و خدمات در اینترنت به طور مناسب کارایی ندارد. سیستم های پرداخت کنونی برای دنیای آنلاین همانند کارت های اعتباری، در سطح گسترده ای به عنوان ابزار پرداختی در اینترنت می باشد، ولی کاربران در این موارد اطمینان، اعتبار، امنیت و ... را مشاهده نمی کنند. سیستم های پرداخت امروزی دور از ایده آل های بازرگانان می باشد، و این به دلیل هزینه بالای معامله، عملیات

کلاهبرداری، و گروه‌های مختلفی که در این فرایند پرداخت مشارکت دارند، است. این مشکلات منجر به بی‌میلی مشارکت کاربران در فعالیت‌های تجارت الکترونیک شده، و این شرایط به نوبه خود، بازرگانی را که مشتریان بالقوه خود را از دست می‌دهند، تحت تأثیر قرار می‌دهد.

سامانه‌های پرداخت کنونی، که به‌طور ویژه برای اینترنت ایجاد شده‌اند، نمی‌تواند از مشکلات ذکر شده مشابه یا متفاوت اجتناب کند. این موارد منجر به بی‌میلی به کارگیری سیستم‌های پرداخت الکترونیک و دشواری سطح پذیرش سیستم‌های پرداختی توسط مشتریان می‌گردد. نیاز به سیستم‌های پرداخت مناسب و کاربرپسند مشخصاً ضروری می‌باشد. این سیستم‌ها می‌بایست نیاز کاربران و بازرگانان را تأمین کنند، و پتانسیل‌های مربوط به پذیرش این دستگاه‌ها را در بازار کالا نشان دهد. در این حالت امنیت مبحث امنیت معنا پیدا می‌کند. به مرور زمان و با موازی کردن سیستم‌های کامپیوتری و شبکه‌های کامپیوتری، توجه به این مسئله اهمیت بیشتری پیدا کرده و نیازمند روش‌های جدیدی است.

امروزه نیز با فراگیر شدن تلفن همراه، مبحث پرداخت با تلفن همراه نمود پیدا می‌کند. این کتاب، سعی بر این دارد که تمامی مفاهیم را پوشش دهد. امیدواریم مد نظر قرار دادن فاکتورهایی که پذیرش سیستم‌های پرداخت الکترونیک را توسط کاربر تحت تأثیر قرار دهد، مورد بررسی قرار گرفته است. در این بررسی سیستم‌های پرداخت سنتی (نقد) دارای اعتباری و الکترونیک (کارت‌های هوشمند و کارت‌های اعتباری اینترنتی) مدنظر قرار گرفته‌اند.



۱۵	فصل اول کلیات
۱۶	مقدمه
۱۷	انگیزه‌ها و پیشران‌های پرداخت الکترونیکی
۱۸	تراکنش‌ها در سامانه پرداخت
۱۸	ویژگی تراکنش‌ها در سامانه‌های پرداخت
۱۹	ویژگی سامانه‌های پرداخت
۲۱	فصل دوم ویژگی‌های سامانه‌های پرداخت
۲۲	مقدمه
۲۲	پرداخت نقدی
۲۴	پرداخت از طریق بانک
۲۴	پرداخت با چک
۲۵	پرداخت با جابرو و یا انتقال اعتبار
۲۶	پرداخت‌های اتاق تسویه اتوماتیک (ACH)
۲۸	خدمات انتقال سیمی (وایر)
۲۸	پرداخت به‌وسیله کارت
۳۰	پرداخت با کارت اعتباری
۳۲	ترجیحات مشتریان در استفاده از سامانه‌های پرداخت
۳۲	چارچوب رگلاتوری و تنظیم مقررات
۳۵	فصل سوم امنیت پرداخت
۳۶	مقدمه
۳۶	رمزگذاری و رمزگشایی
۳۸	رمزگذاری متقارن داده با کلید خصوصی
۳۹	رمزگذاری کلید متقارن
۳۹	الگوریتم رمزگذاری معمول



۴۲	استاندارد رمزگذاری داده (DES)
۴۶	فرایند رمزگشایی
۴۷	فرایند رمزگذاری و رمزگشایی
۴۷	فرایند رمزگذاری
۴۸	رمزگذاری DES سه‌گانه
۴۹	استاندارد رمزگذاری پیشرفته
۵۱	الگوریتم ES
۵۲	رمز IDEA
۵۳	بختی درباره رمزگذاری با کلید متقارن
۵۴	خلاصه‌سازی یا دیکریپشن
۵۴	تابع Hash
۵۵	الگوریتم درهم‌سازی یا Hashing
۵۶	عملکرد تابع Hash
۵۶	MD5
۵۶	الگوریتم MD5
۵۹	SHA
۶۰	کریپتوس
۶۳	نحوه تهیه بلیط
۶۴	رمزگذاری نامتقارن با کلید عمومی
۶۵	ویژگی‌های رمزگذاری نامتقارن
۶۹	امضای دیجیتال
۷۰	مراجع ذی‌صلاح صدور گواهی
۷۰	گواهی سلسله‌مراتبی
۷۱	امضای دوتایی (مثال)
۷۲	جلوگیری از تکرار (Nonces)

فصل چهارم سامانه‌های مبتنی بر کارت اعتباری

۷۳	مقدمه
۷۴	نیازمندی‌های پرداخت‌های الکترونیکی
۷۴	خواص تراکنش‌های الکترونیکی
۷۵	پذیرش سامانه پرداخت پس از پیاده‌سازی
۷۵	انواع کارت‌ها
۷۶	انواع حافظه و ظرفیت کارت‌ها
۷۷	کارت جاوا
۷۸	ویژگی کارت جاوا
۷۹	سامانه کارت اعتباری
۸۲	مراحل پرداخت با کارت اعتباری
۸۳	تراکنش‌های کارت اعتباری
۸۵	پرداخت با کارت اعتباری به کمک پروتکل لایه سوکت امن
۸۹	پروتکل تراکنش‌های الکترونیکی امن
۸۹	ویژگی‌های پروتکل SET
۹۰	اصول امضای دیجیتال
۹۲	کارت بدهی ATM
۹۵	استفاده از کارت در دستگاه خودپرداز

فصل پنجم چک‌های الکترونیکی و انتقال بین حساب‌ها

۹۷	مقدمه
۹۸	انتقال وجه بین سامانه‌های متمرکز
۹۹	واریز وجه به حساب
۱۰۰	انتقال به حساب با تشخیص هویت
۱۰۵	برداشت وجه از سامانه
۱۰۹	مدل‌های تجاری



۱۱۰	FSTC Payment Initiatives
۱۱۰	چک الکترونیکی
۱۱۳	Financial Services Markup Language
۱۱۴	ویژگی‌های FSML
۱۱۵	بلوک امضاء FSML
۱۱۶	نمونه‌ای از چک الکترونیکی با FSML
۱۱۷	جریان عملیاتی چک الکترونیکی
۱۱۷	سناریو اول : Deposit and Clear
۱۱۸	سناریو دوم : Cash and Transfer
۱۱۹	سناریو سوم : Bank Box
۱۲۰	سناریو چهارم : Fund Transfer
۱۲۰	Swift
۱۲۲	انواع پیام‌های Swift

۱۲۵	فصل ششم پرداخت نقدی الکترونیکی
۱۲۶	مقدمه
۱۲۷	سامانه‌های پرداخت نقدی الکترونیکی
۱۲۷	پرداخت نقدی الکترونیکی - ایده‌ی اول
۱۲۸	امضای کور Blind Signature - ایده‌ی دوم
۱۳۳	پرداخت نقدی الکترونیکی (Ecash)
۱۳۴	مدل Ecash
۱۳۵	ذی‌نفعان و وظایف آن‌ها در سامانه Ecash
۱۳۶	سکه‌های Ecash
۱۳۷	کلیدهای سکه
۱۳۹	تقلب در کلید سکه
۱۴۰	جلوگیری از تقلب



۱۴۱	جلوگیری از هزینه مجدد
۱۴۲	مدیریت پایگاه داده
۱۴۳	برداشت سکه
۱۴۳	مراحل برداشت سکه
۱۴۵	خرید Ecash
۱۴۶	انجام پرداخت
۱۴۸	نات پرداخت
۱۴۹	مزایای پرداخت
۱۴۹	یکپارچگی با وب
۱۵۰	Ecash در سیستم الکترونیکی
۱۵۱	انتقالات در Ecash
۱۵۱	سکه‌های گم‌شده
۱۵۳	Ecash و بهره‌کاری
۱۵۴	پول جادویی Magic Money

۱۵۵	فصل هفتم سامانه‌های پرداخت خرد
۱۵۶	مقدمه
۱۵۶	Millicent
۱۵۸	مدل Millicent
۱۶۰	جایگزینی خدمات اشتراک
۱۶۲	خرید با Millicent
۱۶۴	Scrip
۱۶۵	ساختار Scrip
۱۶۶	تولید گواهی Scrip
۱۶۷	صحت اعتبارسنجی Scrip
۱۶۷	جلوگیری از هزینه‌ی مجدد



۱۶۸	هزینه‌های محاسباتی
۱۶۸	Scrip روی شبکه
۱۷۳	فصل هشتم تجارت سیار
۱۷۴	مقدمه
۱۷۴	محدودیت تلفن همراه نسبت به PC
۱۷۶	مشاری‌های اینترنت موبایل
۱۷۶	داده‌های اینترنت بر شبکه سلولی
۱۷۷	پروتکل کار بی‌سیم
۱۸۰	کنسرسیوم‌ها در صنعت در رابطه‌های MC
۱۸۰	اپراتورهای شبکه‌های موبایل عنوان بانک
۱۸۱	سامانه‌های پرداخت همراه مبتنی بر حساب شخصی ثالث
۱۸۲	Sonera Mobile Pay
۱۸۳	Pay Box
۱۸۵	سامانه‌های مبتنی بر کارت اعتباری
۱۸۷	Mobile Set