کوپن های الکترونیکی ایمن

چکیده

کوپن‌ها (اوراق بهادار) در بازار جهانی بسیار مشهورند وبطور گسترده ای بمنظور جذب مشتریان جدیدی که به دنبال معاملات هستند وهمچنین بمنظور حفظ مشتریان وفادار استفاده می‌شوند. بطور کلی، اوراق بهاداری که برای مشتریان وفادار هستند، تخفیف بیشتری نسبت به اوراق بهادار مشتریان جدید دارند. بمنظور فرق گذاشتن بین مشتریان جدید و وفادار، ما دو رویکرد متفاوت را ابداع کردیم که به شرکت‌ها اجازه می‌دهد تا انواع مختلفی از کوپن-های الکترونیکی را از طریق شبکه‌ی اینترنت بیسیم صادر نماید. رویکرد اول برای ایجاد اوراق الکترونیکی‌ای که به مشتریان خاص اختصاص ندارد، استفاده شده است. بنابراین، یک کوپن الکترونیکی استفاده نشده، می‌تواند بوسیله هر مشتری‌ای استفاده گردد. این روش برای جذب مشتریان جدید بسیار مناسب است. روش دیگر برای تولید کوپن الکترونیکی‌ای که به مشتریان خاص اختصاص دارد، استفاده می‌شود. لذا کوپن‌های الکترونیکی استفاده نشده، نمی‌تواند توسط مشتریان دیگر مورد استفاده قرار گیرد. این روش ثانویه، بمنظور حفظ مشتریان وفادار بسیار مناسب است. هر دو طرح پیشنهادی برای تجارت الکترونیکی موبایل طراحی شده است وهزینه‌ی فرآوری وپردازش کوپن‌ها را کاهش می‌دهد.

1. مقدمه

با رشد سریع فن آوری شبکه های کامپیوتری، بسیاری از معاملات سنتی به صورت الکترونیکی انجام می شود. بیشتر وبیشتر برنامه‌های کامپیوتری، همانند حراج‌های الکترونیکی، رای‌گیری الکترونیکی، پرداخت‌های الکترونیکی وغیره برای اجرا روی شبکه‌ی اینترنت توسعه یافته‌اند. بعلاوه ی اینترنت، تحولات ارتباطات تلفن همراه، به‌سرعت در حال

تغییر است ومنافع تجاری فراوان‌اند. ارتباطات موبایل، همچون خدمات ارتباط شخصی(PCS) و سیستم جهانی ارتباط موبایل(UMCS) توسعه یافته‌اند و در سراسر دنیا بسیار محبوب شده‌اند. تکنولوژی‌ها برای فراهم کردن ارتباطات ومحاسبات، بطور پویا طراحی شده‌اند. تاکنون، شبکه‌های موبایل بسیاری توسعه یافته شده‌اند؛ همچون GSM، USDC، PDS وغیره. سیستم GSM در حال حاضر در بیش از 70 کشور در سراسر جهان اجرا شده است. علاوه براین، بسیاری از برنامه‌های کاربردی وخدمات، همچون پروتکل برنامه‌ی بی‌سیم(WAP)، کنفرانس از راه دورِ امن، سیستم پرداخت موبایل، برنامه های کاربردی محل آگاهی وغیره فراهم آورده شده است. تجارت تلفن همراه بطور گسترده‌تری در کسب وکار در حال استفاده است و درحال تبدیل شدن به یک موضوع تحقیق بسیار مهم است.

در بازار سنتی، صدور کوپن یک استراتژی مفید و شناخته شده برای افزایش فروش است. با توجه به خط سود، شرکت ها می توانند کوپن های تخفیف، برای رسیدن به مشتریان جدید صادر کنند. علاوه براین، شرکت‌ها همچنین می‌توانند کوپن‌هایی با تخفیف سنگین برای حفظ مشتریان وفادار صدور نمایند. نتایج حاصل از صدور کوپن های الکترونیکی در اینترنت بسیار آشکار است. علاوه براین، اگر ما بتوانیم مفهوم کوپن‌های الکترونیکی را به محیط موبایل اعمال نماییم، می‌توانیم انتظار داشته باشیم که این مهم مشتریان بیشتری را برای خریداری یک محصول جذب خواهد کرد. بنابراین، ایده استفاده از کوپن های الکترونیکی برای تجارت الکترونیکی تلفن همراه مطرح شده است. هدف اصلی استفاده از کوپن‌های الکترونیکی بمنظور دریافت کردن واستفاده نمودن از کوپن‌های موبایل برای مشتریان است. این فناوری به مشتری اجازه می‌دهد تا یک کوپن‌الکترونیکی را از طریق موبایل خود دریافت نماید. سپس مشتری هنگام تصمیم به خرید محصول، کوپن الکترونیکی را برای تاجر ارسال می‌نماید.

اگرچه در فضای الکترونیک، اطلاعات براحتی می‌تواند به سرقت رود یا دستکاری شود. از این رو، چگونگی ساخت یک کانال امن برای انجام معاملات، با استفاده از کوپن‌های الکترونیکی یک موضوع کلیدی در چنین فن آوری است. بنابراین، برخی از نیازمندی های امنیتی برای این تکنولوژی ضروری است. ما خلاصه نیازمندی های امنیتی را برای استفاده از کوپن های الکترونیکی به شرح زیر خلاصه کرده‌ایم:

1. احراز هویت: به منظور جلوگیری مشتری از جعل کوپن های الکترونیکی، منشاء کوپن های الکترونیکی باید معین شود. بنابراین یک تاجر باید توانایی تصدیق اعتبار تمامی کوپن‌های الکترونیکی دریافت شده را داشته باشد.

2. صداقت: به منظور جلوگیری مشتری از اصلاح کوپن های الکترونیکی، تمامیت الکترونیکی کوپن باید نگه داشته شود. بنابراین، یک تاجر باید اطمینان حاصل کند که کوپن¬های الکترونیکی دریافت شده است، اصلاح نشده است.

3. جلوگیری از استفاده مکرر: به منظور جلوگیری از استفاده نامحدود از کوپن های الکترونیکی، تعداد کوپن های الکترونیکی صادره باید محدود شود. بنابراین، سیستم باید مشتری را از استفاده دو باره از همان کوپن الکترونیکی بازدارد.

علاوه بر الزامات امنیتی، عملکرد کوپن های الکترونیکی نیز بسیار مهم است. با توجه به فضای حافظه کوچک و قابلیت های محاسباتی پایین تجهیزات الکترونیکی تلفن همراه، هزینه پردازش الکترونیکی کوپن، از جمله هزینه های محاسباتی، حافظه فضای بالای سر، و هزینه های ارتباطی، باید تا حد امکان کاهش یابد.

به منظور برآوردن این شرایط، برخی از تکنیک های رمزنگاری کارآمد مانند توابع هش می تواند ما را در طراحی چنین طرح الکترونیکی کوپن کمک نماید. به عنوان مثال، به منظور افزایش فروش و جذب مشتریان جدید، شرکت ها ممکن است آرزو کنندکه یک مشتری می تواند یک کوپن الکترونیکی استفاده نشده را به مشتری بالقوه دیگری فوروارد نماید، در صورتی که آن مشتری نخواهد از آن استفاده کند. از سوی دیگر، به منظور حفظ مشتریان وفادار، شرکت ممکن است ای-کوپنهای ویژه‌ای را به مشتریان وفادارصادر کند. ای-کوپنهای ویژه معمولا تخفیف قیمت بیشتری دارند یا یک محصول را بصورت رایگان پیشنهاد می‌دهند.

با توجه به دو استراتژی مختلف برای صدور کوپن، ما دو طرح متفاوت عملی را برای ای-کوپن ابداع کردیم که همه‌ی الزامات را ارضا می‌کند. در طرح پیشنهادی اول، کوپن‌های الکترونیکی‌ای که صادر می‌شوند، به مشتری خاصی اختصاص ندارند. لذا، می تواند توسط هر مشتری استفاده شود. در طرح پیشنهادی دوم، ای-کوپن‌هایی که صادر می‌گردد به مشتریان خاصی اختصاص می‌یابد. بنابراین نمی‌تواند توسط هر مشتری استفاده شود. از دانش فعلی مان، ما هنوز هیچگونه طرح مشابهی برای بحث در مورد تمایز بین کوپن‌های الکترونیکی‌ای که به مشتریان خاص،

اختصاص ندارد وکوپن‌هایی که به مشتریان وفادار خاصی اختصای می‌یابد، پیدا نکرده‌ایم. بقیه این مقاله به شرح زیر سازماندهی شده است:

در بخش 2، فن‌آوری کد تایید هویت پیغام معرفی خواهد شد. این تکنولوژی بعدا در طرح‌های پیشنهادی ما استفاده می‌شود. چارچوب سیستم و نمادهای مورد استفاده در سراسر بقیه مقاله در بخش 3 معرفی شده است. در بخش 4، ما طرح پیشنهادی اول را آورده‌ایم که برای صدور کوپن‌های الکترونیکی‌ای است که به مشتریان خاص اختصاص ندارد. در بخش 5، ما طرح پیشنهادی دوم را برای صدور ای-کوپن‌هایی که به مشتریان خاصی اختصاص دارد، آورده‌ایم. در بخش 6، خواص و عملکرد طرح های ما آزموده می‌شود. بخش 7 این مقاله را نتیجه گیری می‌کند.

2.کد تایید پیام

کد تایید پیام (MAC) یک فن آوری رمزنگاری مفید است که به طرح های پیشنهادی ما مفید خواهد بود است. قبل از معرفی MAC، ما ابتدا تکنولوژی تابع هش یک-طرفه را بیان خواهیم کرد. تابع هش یک طرفه، معمولا به تایید درستی یک پیام اعمال می‌شود. برای مثال، MD5 یک تابع یک طرفه هش مشهور است. متن ورودی آن یک بلوک 512 بیتی است. پس از پردازش با MD5، خروجی مجموعه ای از چهار بلوک 32 بیتی است. MD5 می‌تواند ورودی طول دلخواهی را گرفته و خروجی‌ای از طول ثابت را بازگرداند. علاوه براین، می‌تواند نتیجه‌ی یک طرفه ومقاوم در برابر ضربه را ایجاد نماید. ویژگی‌های این تابع هش یک طرفه، در ادامه خلاصه شده است:

1. با توجه به یک طول دلخواه ورودی، خروجی آن را همیشه یک طول ثابت می‌دهد.
2. با دادن یک ورودی، بدست آوردن خروجی از طریق تابع آسان است.
3. از یک خروجی، بدست آوردن ورودی دشوار است.
4. با دادن یک ورودی، پیدا کردن ورودی دیگر دشوار است؛ همچون دو ورودی‌ای که خروجی یکسان دارند.

مزایای استفاده از تابع هش یک طرفه، سرعت بالا واجرای آسان با استفاده از نرم‌افزار یا سخت‌افزار است.

کد تایید پیام، یک تابع هش یک طرفه‌ی خاص است. MAC یک تابع هش یک طرفه‌ی وابسته به کلید است. ورودی این تابع یک پیام M، ویک کلیدK وخروجی یک پیام خلاصه است. این همان ویژگی های تابع هش یک طرفه را داراست، اما با یک کلید تکمیل شده است تا از فردی که سعی در جعل مقدار هش دارد جلوگیری شود. کاربری که صاحب کلید است می‌تواند به آسانی مقدار هش را تایید نماید، در صورتی که دیگران نمی‌توانند. MAC فن آوری رمزنگاری کارآمد است که درستی واحراز هویت را با هزینه‌های عملیاتی پایین‌تر بدست می‌دهد. استاندارد ISO الگوریتمMAC در مرجع 1 بیان شده است. این آسان‌ترین راه اجرای تابع MACاست . توابع رمزنگاری FEAL یا DES در این الگوریتم استفاده شده اند. پس از پردازش با استفاده از تابع hash یک طرفه، مقدار هش با استفاده از چنین الگوریتم رمزنگاری‌ای، رمزگذاری شده است. از این رو هزینه محاسبات MAC، محاسبه هش و رمزنگاری کلید متقارن است. این فن آوری برای استفاده در سیستم های کوپن الکترونیکی مناسب است.

3. چهارچوب سیستم ونمادها

طرح کوپن الکترونیکی ارائه شده از سه نهاد تشکیل شده است: یک شرکت، مشتریان، و بازرگانان. شرکت، نهادی است که کوپن‌های الکترونیکی را صادر می‌کند و آن‌ها را از طریق یک شبکه بی‌سیم اینترنت، به مشتریان بالقوه توزیع می‌نماید. پس از دریافت یک ایمیل کوپنی، مشتری می تواند کوپن الکترونیکی را به یک تاجر از طریق موبایل خود فوروارد کرده ومحصول را خریداری کند. یک شرکت ممکن است هیچ، یک یا چندین تاجر داشته باشد. یک تاجر، عضوی از شرکت است که مبادرت به فروش محصولات می‌کند. تاجر دارای یک دستگاه پایانه‌ی فروش الکترونیکی است که توسط شرکت توزیع می‌شود. یک تراشه مقاوم به دستکاری، مانند کارت هوشمند یا SIM کارت، به داخل دستگاه تعبیه شده وشامل کلید امنیتی شرکت وتابع اعتبار سنجی است. تراشه مدار مجتمع در دستگاه، از اطلاعات ذخیره شده در برابر کپی یا نشت، در یک محل مخفی محافظت می‌کند. در طی فرآیند تأیید، دستگاه هیچ اطلاعات محرمانه را فاش نمی‌کند. علاوه بر این، شرکت یک سیستم پایگاه داده ایجاد می‌کند که هر کوپن الکترونیکی صادر شده را ذخیره می‌کند و چک می‌کند که آیا کوپن تا قبل ا استفاده شده است یا نه. این

مکانیزم می‌تواند از استفاده نامحدود همان کوپن الکترونیکی جلوگیری کند. پس از دریافت یک ای-کوپن، تاجر ابتدا اعتبار کوپن را از طریق دستگاه پایانه‌ی فروش تایید می‌کند وسپس به پایگاه داده شرکت متصل شده وبررسی می‌کند که آیا از کوپن الکترونیکی دوبار استفاده شده است. ارتباط بین شرکت و بازرگانان می تواند یک شبکه مالی باشد. چارچوب سیستم کوپن الکترونیکی مطرح شده در شکل 1 نشان داده شده است. خطوط نقطه چین نشان دهنده شبکه های بی سیم است. خط توپر نشان دهنده شبکه های مالی است.

قبل از بیان روند طرح‌هایمان، ما ابتدا باید نمادگذاری‌های زیر را معرفی نماییم:

• MAC(K,M): تابعی برای کد تایید هویت پیام است. ورودی این تابع یک پیام M و یک کلید Kاست. خروجی این تابع یک پیام خلاصه با طول ثابت است.

• IDC: هویت منحصر بفرد هر مشتری مانند شماره موبایل است.

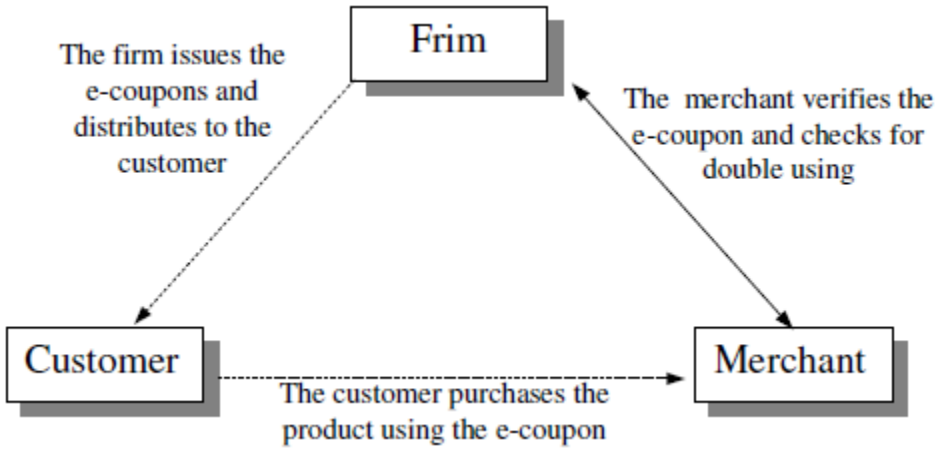
• KF/KC: کلید مخفی شرکت/مشتری است هنگامی که

• PRODUCT: اطلاعات محصولات تخفیف دار، مانند شماره‌های ID محصول.

• SER: یک شماره‌ی سریال منحصر بفرد برای هر کوپن الکترونیکی.

• VDATE: یک تاریخ معتبر برای هر کوپن الکترونیکی.

• COUPON: کوپن الکترونیکی صادر شده که شامل پیام‌های PRODUCT,SER و VDATE.



شکل1. چارچوب کوپن الکترونیکی

4. طرح اول: کوپن‌هایی که به مشتریان خاص اختصاص ندارند

در این بخش، ما باید ابتدا، طرح اول را که کوپن های الکترونیکی را که به مشتریان خاص اختصاص ندارد، صادر می‌کند، توصیف نماییم. چنان‌که کوپن می‌تواند توسط دیگر مشتریان بالقوه استفاده شود، اگر مشتری‌ای که کوپن الکترونیکی دریافت می‌کند، از آن استفاده نکند. طرح ما باعث استفاده از MAC به عنوان یک عملیات اساسی می‌شود. این فرایند در طرح ما شامل سه مرحله است: صدور الکترونیکی کوپن و فاز توزیع، فاز خرید، و فاز امنیتی. این مراحل به شرح زیر است.

1. صدور الکترونیکی کوپن و فاز توزیع: شرکت ابتدا روی تعداد کوپن‌های الکترونیکی‌ای که باید برای یک محصول صادر گردد، تصمیم می‌گیرد. فرض کنید که تعداد کوپن‌هایی که باید صادر شود N است. سپس کوپن های الکترونیکی می‌تواند توسط شرکت با استفاده از فرمول زیر تولید تولید گردد:

$$H_i = MAC(K_F, PRODUCT \| SER_i \| VDATE), \quad (1)$$

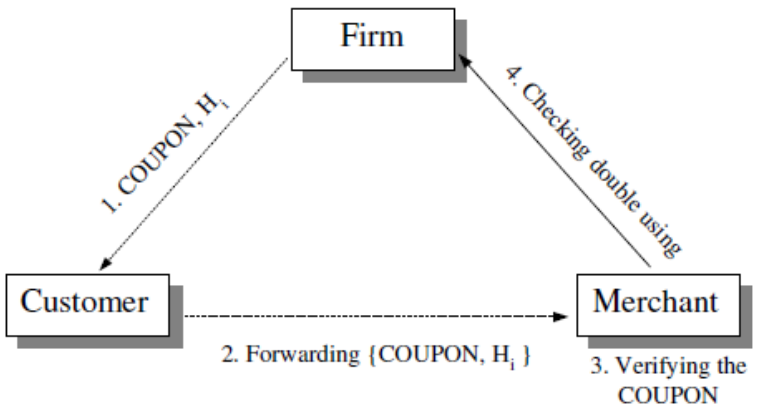
هنگامی که i از 1 تا n است ونماد II نشان‌دهنده‌ی تمرکز است. بعد ازآن، شرکت کوپن‌های الکترونیکی $\{\hat{PRODUCT}, SER_i, VDATE\}$ را با H_i به مشتری بالقوه C_i، از طریق یک شبکه‌ی وایرلس توزیع می‌کند.

2.فاز خرید: بعد از دریافت کوپن‌های الکترونیکی، مشتری می‌تواند کوپن الکترونیکی $\{\hat{PRODUCT}, SER_i, VDATE\}$ وH_i را در صورتی که بخواهد محصول را با تخفیف قیمت خریداری نماید، به تاجر فوروارد نماید.

3. مرحله تایید: پس از دریافت موفقیت آمیز کوپن الکترونیکی، تاجر ابتدا تاریخ کوپن را برای بررسی صحت آن، چک می‌کند. اگر کوپن الکترونیکی هنوز معتبر باشد، تاجر از دستگاه پایانه‌ی فروش استفاده می‌کند تا تایید نماید که آیا رابطه پیش‌رو $MAC(K_F, PRODUCT \| SER_i \| VDATE)$ صحیح است یا نه، بطوریکه کلید محرمانه‌ی شرکت K_F در دستگاه ذخیره شده است واطلاعات PRODUCT، SER_i وVDATEرا از پیغام دریافتی، بدست می‌آورد. اگر رابط ارضا گردد، {PRODUCT _SERi_V DATE} بعنوان یک کوپن معتبر پذیرفته می‌شود. سپس تاجر کوپن الکترونیکی را بمنظور اینکه ببیند از آن قبلا استفاده شده است یانه، به شرکت ارسال می‌کند. شرکت محل

ثبت کوپن را طبق SER_i پیدا می‌کند وکوپن را برای بررسی این‌که قبلا استفاده شده است یا نه، چک می‌کند. اگر بررسی نشان دهد که کوپن الکترونیکی معتبر است، شرکت یک پیام تایید به تاجر می‌فرستد وکوپن را با عنوان استفاده شده ثبت می‌نماید. اگر بررسی نشان دهد که کوپن الکترونیکی معتبر نیست، این بدان معنی است که بیش از یکبار استفاده شده است. تاجر این معامله را نادیده می‌گیرد ویک پیغام رد به مشتری ارسال می‌کند.

در این طرح، کوپن‌های الکترونیکی صادر شده، به مشتریان خاصی با استفاده‌ی شخصی تعلق نمی‌گیرد. بنابراین اگر یک مشتری از کوپن استفاده ننماید، کوپن الکترونیکی می‌تواند به مشتری بالقوه‌ی دیگری فورواد شود. شرکت تنها از کوپن‌ها در برابر استفاده دوباره جلوگیری می‌نماید. اگر شرکت اهمیتی به کوپن‌های الکترونیکی استفاده شده، بدون محدودیت ندهد، فرآیند بررسی اینکه آیا ای-کوپن استفاده شده است یا نه، نادیده در نظر گرفته می‌شود. شکل 2فرآیند طرح پیشنهادی اول را نشان می‌دهد. خط چین نشان دهنده شبکه های بی سیم و خط توپر نشان دهنده شبکه های مالی است.



شکل2. فرآیند طرح 1

5. طرح2: کوپن‌های الکترونیکی که به مشتریان خاص اختصاص دارند

متفاوت از طرح 1، ای-کوپن‌های صادره با استفاده از این طرح به مشتریان خاص اختصاص داده شده‌اند. بنابراین، کوپن های الکترونیکی نمی تواند بصورت اتفاقی توسط دیگر مشتریان بالقوه استفاده شود،اگرکه مشتری کوپن الکترونیکی‌ای را دریافت می‌کند، از آن استفاده نمی‌کند. طرح 2 بصورت زیر توصیف می‌شود:

1. مرحله ثبت نام: مشتریان وفادار معمولا برای عضویت در شرکت دعوت می‌شوند. ابتدا، مشتری اطلاعات شناسایی خود IDS را، همچون شماره موبایل یا چیز دیگر به‌شرکت ارسال می‌کند. سپس شرکت یک کلید محرمانه K_c را برای احراز هویت مشتری، با استفاده از فرمول پیش رو تولید می‌نماید:

$$K_C = MAC(K'_F, ID_C), \qquad (2)$$

درحالیکه K'_F کلید مخفی دیگر شرکت است که کلید مخفی مشتری را تولید می‌کند. در پایان، شرکت کلیدهای مخفی K_c را به شیوه‌ای بسیار امن به مشتری تحویل می‌دهد. این مرحله فقط یک بار انجام می‌شود.

2. مرحله صدور کوپن‌الکترونیکی وتوزیع: شرکت تصمیم می‌گیرد که چه کسی کوپن را دریافت خواهد کرد وچه تعداد کوپن الکترونیکی برای یک محصول صادر خواهد شد. فرض کنید که تعداد کوپن‌هایی که باید صادر شود nو هویت‌های دریافت کنندگان $ID_{C_1}, ID_{C_2}, \cdots, ID_{C_n}$ باشد. سپس، کوپن‌ها، بوسیله‌ی رابطه‌ی زیر توسط شرکت تولید می‌شود:

$$H_i = MAC(K_F, PRODUCT \| SER_i \| \\ VDATE \| ID_{C_i} \| S_i), \qquad (3)$$

درحالیکه S_i برابر است با:

$$\begin{aligned} S_i &= MAC(MAC(K'_F, ID_{C_i}), SER_i) \quad (4) \\ &= MAC(K_{C_i}, SER_i), \end{aligned}$$

و i از 1 تا n است. سپس، شرکت کوپن‌ها را $\{PRODUCT, SER_i, VDATE\}$با H_i به مشتریان خاصی توسط شبکه‌ای بیسیم توزیع می‌نماید.

1. فاز خرید: بعد از دریافت کوپن‌های الکترونیکی$\{PRODUCT, SER_i, VDATE\}$و H_i، مشتری ابتدا از کد خود K_{Ci} برای محاسبه‌ی S_i استفاده می‌کند بطوریکه $S_i = MAC(K_{C_i}, SER_i)$. سپس مشتری کوپن را $\{PRODUCT, SER_i, VDATE\}$بهمراه S_i، ID_{ci} وH_i برای تاجر می‌فرستد.

2. مرحله تایید: پس از دریافت الکترونیکی کوپن، تاجر اول چک می‌کند که آیا ا تاریخ کوپن معتبر است و پس از آن بررسی کند که آیا رابطه

$$H_i = MAC(K_F, PRODUCT\| \quad (5)$$
$$SER_i\|VDATE\|ID_{C_i}\|S_i)$$

ارضا می‌گردد یا نه، که ID_c می‌تواند توسط شماره موبایلی که در پیغام ورودی وجود دارد، بدست آید. اگر اعتبار سنجی نشان از صحت رابطه دهد، $\{PRODUCT, SER_i, VDATE\}$بعنوان یک کوپن معتبر تایید می‌گردد. سپس تاجر کوپن$\{PRODUCT, SER_i, VDATE\}$، ID_c وS_i را به شرکت برای بررسی اینکه آیا قبلا استفاده شده است یانه، می فرستد. این مرحله همانند طرح1 است. اگر کوپن الکترونیکی معتبر باشد، شرکت یک پیغام تایید را برای تاجر می‌فرستد وتاجر خرید مشتری را تایید می‌کند.

در این طرح، کوپن های الکترونیکی صادره به مشتریان خاص برای استفاده اختصاص داده شده است. بنابراین، تنها زمانی که مشتری مشخص از کلید مخفی خود، برای محاسبه Si معتبر استفاده می‌کند وکوپن را با استفاده از شماره موبایل خود ارسال می‌کند، کوپن الکترونیکی می‌تواند استفاده شود.

6. بحث

کوپن های سنتی نیاز به پاسخگویی به ملزومات امنیتی دارند: (1) احراز هویت، (2) صداقت و3) استفاده‌ی یکباره. با این حال، طراحی کوپن های الکترونیکی بیشتر پیچیده است. علاوه بر سه تابع اصلی کوپن‌های سنتی، آنها همچنین نیاز به ارضا ضروریات خاص برنامه‌های کاربردی الکترونیکی کوپن‌ها دارند. در این بخش، ما توابع وعملکرد قدرت طرح پیشنهادی را تجزیه و تحلیل می‌کنیم.

A. تحلیل توابع امنیتی

1. احراز هویت: در محیط الکترونیکی، مشتری قادر به ایجاد یک کوپن الکترونیکی و ارسال آن به یک تاجراست. این خطرناک است و بنابراین ما باید، تصدیق اعتبار تمام کوپن‌های دریافتی را احراز نماییم. این شرط، احراز هویت نامیده می‌شود. طرح پیشنهادی ما با این شرط، با اجازه دادن به یک تاجر برای تعیین منشاء کوپن های الکترونیکی مطابقت دارد. در صدور الکترونیکی کوپن وفاز توزیع طرح‌های ما، یک کوپن الکترونیکی توسط معادلات 1 و3 تولید می‌شود.

یک ای-کوپن معتبر تنها می‌تواند بوسیله‌ی شرکت واقعی، با کلید مخفی تولید گردد. هر کاربر دیگری در سیستم، به هیچ وجه نمی‌تواند یک ای-کوپن معتبر را بدون آگاهی از کلید مخفی شرکت واقعی تولید نماید. این امر برای مشتری‌ای که سعی در جعل یک کوپن الکترونیکی، از طرف شرکت دارد غیر ممکن است؛ چراکه جاعل درمی‌یابد که دستیابی به یک H_i معتبر سخت است.

بنابراین، یک تاجر می تواند اعتبار الکترونیکی کوپن در این سیستم را بررسی کند. علاوه بر این، در طرح 2، یک تاجر نیز باید این را که آیا کوپن الکترونیکی دریافتی از یک مشتری خاص است، تایید کند. در مرحله‌ی تایید طرح 2، S_i از معادله‌ی 4 با استفاده از کلید مخفی K_{Ci} تولید می‌شود. کلیدهای مخفی در سیم‌کارت ذخیره می‌شود که در داخل موبایل مشتری تعبیه شده است. سیم‌کارت در برابر دستکاری مقاوم است واز داده‌هایی که قابل خواندن نیستند محافظت می‌کند. علاوه بر این، ما می‌توانیم شرکتی را که کلید مخفی مشتری را صادر می‌کند، بعنوان حزب معتمد فرض کنیم. چون‌که کلید مخفی $K_{C_i} = MAC(K'_F, ID_{C_i})$ با کلید مخفی شرکت K'_F تولید می‌شود، هیچکس نمی‌تواند کلید مخفی معتبر مشتری را استخراج کند. لذا، تاجر می‌تواند مطمئن باشد که ای-کوپن، بوسیله‌ی مشتری خاصی ارسال شده است اگر تایید اعتبار در رابطه‌ی 5 صحیح باشد.

بنابراین، طرح های پیشنهادی در برابر جعل محافظت می‌کند. هر جعل یا تقلبی از ای-کوپن می‌تواند بصورت موفق آمیزی در طرح‌های پیشنهادی ما شناسایی شود.

2. صداقت: اسناد الکترونیکی می تواند به راحتی به ویژه هنگامی که در حمل و نقل است تغییر یابد. بنابراین، هنگامی که یک تاجر، یک کوپن الکترونیکی و H_i مرتبط با آن را دریافت می‌نماید، ما باید مطمئن باشیم که ای-کوپن‌های دریافتی اصلاح نشده باشند. این شرط، صداقت نامیده می‌شود. برای مثال، فردی ممکن است اطلاعات مربوط به PRODUCTیک کوپن را با یکی دیگر جایگزین کند. طرح‌های پیشنهادی ما نیز صداقت ای-کوپن‌های دریافتی را تایید می‌کند.

فرض کنید که یک مشتری سعی در تغییر PRODUCT، برای تغییر در اطلاعات محصول یا تغییر در VDATE برای تمدید مدت اعتبار داشته باشد. اصلاح نمی‌تواند موفق باشد، چراکه مشتری نمی‌تواند H_i معتبر را برای ای-کوپن‌های اصلاح شده تولید نماید. اصلاح نمی‌تواند مرحله‌ی تایید طرح‌های پیشنهادی ما را بگذراند.

در طرح 2، صداقت نیز حفظ می‌شود. اگر یک مشتری سعی در تغییر SER برای استفاده از یک ای-کوپن بیشتر از یکبار داشته باشد، این اصلاح نمی‌تواند موفقیت آمیز باشد. اگر چه شاید یک مشتری بتواند S_i را برای SER اصلاح شده استخراج کند، اما نمی‌تواند H_i معتبر را برای اطلاعات اصلاح شده استخراج کند. لذا، صداقت در طرح‌های ما ارضا می‌گردد.

3. استفاده‌ی یکباره: بمنظور جلوگیری از استفاده نامحدود کوپن‌ها، شرط استفاده‌ی یکباره باید ارضا شود. در طرح‌های ما، یک تاجر می‌تواند توسط بررسی پایگاه داده‌ی شرکت اطمینان یابد که کوپن‌های دریافتی فقط یکبار استفاده شده است. اگر یک مشتری یک ای-کوپن را بمنظور استفاده‌ی مجدد کپی کند، شرکت براحتی می‌تواند مشکل را بوسیله‌ی دیتابیس خودش پیدا کند. بنابراین، هرکه سعی در تکرار استفاده از یک ای-کوپن را داشته باشد، خنثی خواهد شد.

B. آنالیز عملکرد

در این زیربخش، ما عملکرد طرح‌هایمان را بررسی خواهیم کرد.

1) هزینه محاسباتی: MAC عملیات اصلی برای تولید و تایید ای- کوپن‌ها، در طرح های پیشنهادی ما است. از این رو تعداد عملیات MAC برای تعیین هزینه محاسباتی می‌تواند استفاده شود. بر طبق استاندارد ISO یک الگوریتم MAC، الگوریتم MAC از تابع رمزنگاری DES برای رمزنگاری مقدار hash که با استفاده از تابع هشMD5 محاسبه می‌شود، استفاده می‌کند. بنابراین هزینه‌ی محاسباتی MAC یک محاسبه تابع هش است ویک محاسبه‌ی تابع رمزنگاری. جدول 1 تعداد امضا کلید عمومی، رمزنگاری کلید متقارن وتابع هش یک-طرفه است که می تواند در

هر ثانیه در یک ایستگاه کاری معمولی انجام دهد. با توجه به نتایج شبیه سازی، ما کشف می‌کنیم که یک طرفه تابع هش و رمزگذاری کلید متقارن بسیار ارزان تر از امضای کلید عمومی است.

جدول 2 هزینه های محاسباتی برای هر نهاد در طرح های پیشنهادی ما نشان می دهد. در این جدول، F نشان دهنده شرکت، C نشان دهنده مشتری، و M نشان دهنده بازرگان است. ما می توانیم ببینیم که طرح های پیشنهادی در واقع نیاز به هزینه های محاسباتی بسیار کم دارند. علاوه بر این، قابلیت محاسباتی تلفن همراه مشتری معمولا کوچکتر از قابلیت محاسباتی دستگاه تاجر است. بنابراین، یک طرح عملی باید بار را از تلفن همراه مشتری کاهش دهد. طرح‌های پیشنهادی ما این وضعیت واقعی را برآورده می‌سازد.

TABLE I. THE COMPARISONS OF THE COMPUTATIONAL SPEED

Operation	Number per second
Public key signature (1024 bits RSA)	2
Symmetric key encryption (DES)	2,000
One-way hash function (MD5/SHA)	20,000

TABLE II. THE SUMMARY OF THE COMPUTATIONAL COST FOR THE ENTITIES IN THE PROPOSED SCHEMES

Schemes	Scheme 1	Scheme 2
Symmetric key encryption		
F	1	2
C	0	1
M	1	1
One-way hash function		
F	1	2
C	0	1
M	1	1

2) فضای محاسباتی بالاسری: فضای بالای سر حافظه بستگی به اندازه یک ای-کوپن و مقدار هش مرتبط با آن دارد. از آن‌جا که MD5 بعنوان یک تابع هش در استاندارد ISO الگوریتمMAC درنظر گرفته می‌شود ونیز در طرح های پیشنهادی ما استفاده شده است، اندازه ی ورودی MD5 می‌تواند برای تعیین طول هر متغیر در هر کوپن الکترونیکی استفاده شود. بر طبق استاندارد MD5، متن ورودی یک بلوک 512 بیتی است و خروجی مجموعه ای از چهار بلوک 32 بیتی است. ما می‌توانیم نتایج را به شکل یک مقدار هش 128 بیتی الحاق کنیم.

بنابراین، ما می‌توانیم تعیین کنیم که طول پیغام $\{PRODUCT \| SER \| VDATE\}$ 256 بیت، طول S 128 بیت وطول ID_{Ci} 128 بیت است. البته، ما می‌توانیم بطور منعطفی طول این پیغام‌ها را تعیین کنیم. در طرح 1، چون اندازه‌ی اندازه‌ی متغیرها در متن ورودی MAC در کل کمتر از 512 بیت است، ما می‌توانیم با چند صفر آنها را برای تصحیح سایز ورودی، پد کنیم. بعد از فرآیند MD5، مقدار هش مرتبط Hبرابر 128 بیت است. جدول 3 فضای حافظه مورد نیاز به ترتیب در پایانه های مشتری، تاجر، و شرکت را نشان می دهد. در این جدول، N نشان دهنده تعداد صدور کوپن های الکترونیکی، m نشان دهنده تعداد کوپن های الکترونیکی دریافت شده توسط مشتری، و R نشان دهنده تعداد کوپن های الکترونیکی است که در یک تاجر استفاده می شود. از آنجا که شرکت باید بررسی کند که آیا همان کوپن الکترونیکی در قبل استفاده شده، یک پایگاه داده برای همه‌ی کوپن‌های صادره باید توسط شرکت نگهداری شود. بنابراین، فضای محاسباتی ضروری دیتابیس، بستگی به تعداد کوپن‌های الکترونیکی صادره دارد.

3) هزینه‌های ارتباطی: اندازه‌ی پیغام‌های منتقل شده به‌عنوان هزینه‌ی ارتباطی درنظر گرفته می‌شود. مشابه فضای حافظه‌ی بالاسری، ما می‌توانیم سایز کلی متغیر ها را در یک ای-کوپن برابر 256 درنظربگیریم ومقدار هش مرتبط را برابر 128 بیت. جدول 4 هزینه های ارتباطی برای هر اتصال در طرح های ما را نشان می دهد. در این جدول، F C - بدان معنی است که این شرکت یک پیام به مشتری می فرستد، C -M بدان معنی است که مشتری پیام به تاجر می فرستد و M - F بدان معنی است که تاجر یک پیام به شرکت ارسال میکند.

TABLE III. THE SUMMARY OF THE MEMORY SPACE OVERHEAD FOR THE ENTITIES IN THE PROPOSED SCHEMES

Schemes	Scheme 1	Scheme 2
F	256 bits $\times n$	256 bits $\times n$
C	384 bits $\times m$	384 bits $\times m$
M	384 bits $\times r$	640 bits $\times r$

TABLE IV. THE SUMMARY OF THE COMMUNICATION COST FOR THE CONNECTIONS IN THE PROPOSED SCHEMES

Schemes	Scheme 1	Scheme 2
F-C	384 bits	384 bits
C-M	384 bits	640 bits
M-F	256 bits	256 bits

7. نتیجه‌گیری

در این مقاله، ما دو طرح جدید برای صدور کوپن‌های الکترونیکی ارایه کردیم: یک روش کوپن‌های الکترونیکی را که به مشتریان خاص تعلق ندارد، صادر می‌کند؛ دیگری کوپن‌های الکترونیکی را که به مشتریان خاص تعلق دارد، صادر می‌کند. علاوه بر برقراری سه شرط امنیتی، 1)احراز هویت،2)صداقت 3) استفاده‌ی یکباره، طرح‌های بیان شده، ویژگی‌های مطلوب زیر را داراست:

1. هزینه‌ی محاسباتی پایین
2. فضای پایین حافظه‌ی بالاسری
3. هزینه‌ی ارتباطی پایین

بنابراین، طرح های پیشنهادی بسیار کارآمد و عملی است. آنها نه تنها می‌توانند در اینترنت مورد استفاده قرار گیرد، بلکه به خصوص برای استفاده در شبکه های بی سیم مناسب هستند. ما امیدواریم که طرح‌های پیشنهادی بتواند تجارت الکترونیکی موبایل را توسعه دهد.

REFERENCES

[1] ISO/IEC 9797, "Data cryptographic techniques-data integrity mechanism using a cryptographic check functionemploying a block cipher algorithm," Internal Organization for Standardization.

[2] R. Anand, M. Kumar, and A. Jhingran, "Distributing e-coupons on the Internet," Proceedings of the 9th Conference on Internet Society (INET'99), San Jose, 1999.

[3] R. Cramer, R. Gennaro, and J. Borrell, "A secure and optimally efficient multi-authority election scheme," Advances in CryptologyEUROCRYPT'97, Lecture Notes in Computer Science, vol. 1233, pp. 103–117, 1997.

[4] I. B. Damgard, "A design principle for hash functions," Advances in Cryptology-CRYPTO'89, Lecture Notes in Computer Science, vol. 0435, pp. 416–427, 1989.

[5] D. W. Davies, "A message authentication algorithm suitable for a mainframe computer," Advances in Cryptology-CRYPTO'84, Lecture Notes in Computer Science, vol. 0196, pp. 393–400, 1984.

[6] R. Garg, P. Mittal, V. Agarwal, and N. Modani, "An architecture for secure generation and verification of electronic coupons," Proceedings of 2001 USENIX Annual Technical Conference, pp. 51–63, Boston, USA, 2001.

[7] WAP forum, "Wireless applicaion protocol," see http://www.wapforum.org.

[8] M. Hendry, Smart card security and applications, Artech House, 1997.

[9] K. F. Hwang, I. C. Lin, and C. C. Chang, "A credit card-based mobile payment system," Proceedings of 2002 International Conference on Information Security (InfoSecu02), pp. 82–88, Shanghai, China, July 2002.

[10] M. S. Hwang, I.C. Lin, and L. H. Li, "A simple micro-payment scheme," The Journal of Systems and Software, vol. 55, no. 3, pp. 221–229, 2001.

[11] M. S. Hwang, E. J. L. Lu, and I. C. Lin, "Adding timestamps to the secure electronic auction protocol," Data and Knowledge Engineering, vol. 40, no. 2, pp. 155–162, 2002.

[12] M. S. Hwang and W. P. Yang, "Conference key distribution schemes for secure digital mobile communications," IEEE Journal on Selected Areas in Communications, vol. 13, no. 2, pp. 416–420, Feb. 1995.

[13] H. W. E. Jones, A. C. Watson, and T. J. O'Neill, "Vehicle security using smartcards," Security Journal, vol. 10, no. 2, pp. 79–87, 1998.

[14] H. Maass, "Location-aware mobile applications based on directory services," Mobile Networks and Applications, vol. 3, no. 2, pp. 157–173, Aug. 1998.

[15] R. C. Merkle, "One way hash function and DES," Advances in Cryptology-CRYPTO'89, Lecture Notes in Computer Science, vol. 0435, pp. 428–446, 1989.

[16] R. C. Merkle, "A fast software one-way hash function," Journal of Cryptology, vol. 3, no. 1, pp. 43–58, 1990.

[17] B. Schneier, Applied cryptography, John Wiley and Sons, second edition edition, 1996.

[18] S. Suzuki and K. Nakada, "An authentication technique based on distributed security management for the global mobility network," IEEE Journal on Selected Areas in Communications, vol. 15, no. 8, pp. 1608–1617, Oct. 1997.

[19] C. T. Wang, C. C. Chang, and C. H. Lin, "A new micro-payment system using general payword chain," Electronic Commerce Research, vol. 2, no. 2, pp. 159–168, 2002.