هفتمین همایش سالانه
بانکداری الکترونیک
و نظام‌های پرداخت
نوآوری، بازیگران جدید و کارآیی در کسب وکار مالی
تهران، مرکز همایش‌های بین‌المللی برج میلاد - ۲و۳ بهمن ۱۳۹۶
7th Annual Conference
on Electronic Banking
and Payment Systems

ارایه یک زیر ساخت امن یکپارچه برای پرداخت بانکی مبتنی بر موبایل

Present an Integrated Secure Infrastructure for Mobile Banking

حمیده فلاح، آزمایشگاه رایانش ابری و خدمات ارزش افزوده دانشگاه الزهرا (fallah@ossl.ir)
رضا عزمی، دانشگاه الزهرا (azmi@alzahra.ac.ir)
بشری پیشگو، آزمایشگاه رایانش ابری و خدمات ارزش افزوده دانشگاه الزهرا (boshra.pishgoo@ossl.ir)

چکیده (فارسی)

رشد روزافزون روش‌های پرداخت بانکی از یک سو و گستردگی استفاده از تلفن همراه از سویی دیگر، بهره‌گیری از امکانات پرداخت مبتنی بر تلفن همراه را با اقبال روز افزونی روبرو ساخته است. استفاده از سرویس‌های موبایلی برای انجام تراکنشات مالی، علیرغم مزایای فراوان، بدون در نظر گرفتن مسائل امنیتی، با چالش‌های فراوانی روبرو می‌باشد. از جمله‌ی این چالش‌ها می‌توان به امنیت دستگاه تلفن همراه شامل سخت‌افزار، سفت‌افزار و سیستم‌عامل، امنیت برنامه‌های کاربردی و نحوه‌ی نصب و تأیید آن‌ها و آسیب‌پذیری‌های موجود در زیرساخت شبکهٔ سیار و یا نقاط ضعف امنیتی مرتبط با ساختار پروتکل‌های مورد استفاده در این نوع پرداخت‌ها، اشاره نمود. با توجه به مسائل مذکور، هدف مقالهٔ حاضر، ارائه‌ی یک زیرساخت امن یکپارچه بر روی بستر مخابرات سیار به منظور امن‌سازی بستر اصلی روش‌های پرداخت موبایلی می‌باشد.

کلید واژه:

امنیت پرداخت، پرداخت مبتنی بر موبایل، سیم‌کارت، مدیر سرویس قابل اعتماد

چکیده (انگلیسی)

Exponential growth in types of bank payments and use of mobile phones, has made payments based on mobile phones, very popular. Using mobile services to perform financial transactions, without considering security issues, would lead to challenges. Some of these challenges are mobile phones hardware , firmware and Operating System security,applications security and the way they get installed and verified, vulnerabilities that may exist in mobile network infrastructure or even security weaknesses in payment protocols.

Considering above mentioned issues, this papers aims on proposing a secure and integrated infrastructure over mobile telecommunication platform, which secures the main platform of mobile payments.

Key Words:

Payment Security, Payment based on mobile, SIM Card, TSM.

۱- مقدمه

امروزه مکانیزم‌های پرداخت مبتنی بر موبایل، با اقبال زیادی روبرو می‌باشند اما آنچه مسلم است این است که این مکانیزم‌ها بدون فراهم‌سازی محیطی امن برای آنها، قابل قبول نمی‌باشند. از اینرو برای بررسی و ارائه‌ی زیرساخت امن پرداخت موبایلی، ابتدا باید روش‌های پرداخت موبایلی را بررسی نمود. پرداخت‌های موبایلی در چهار دستهٔ عمده شامل صورت‌حساب مستقیم اپراتور[1]، کیف پول موبایل، پرداخت‌های وب موبایل (WAP) و پرداخت‌های NFC قابل تفکیک می‌باشند [۱۱].

در پرداخت نوع اول که صورت حساب مستقیم اپراتور نام دارد و می‌تواند از هریک از کانال‌های sms، ussd و wap صورت گیرد، هزینه‌ی خرید در صورتحساب تلفن ماهانه اضافه شده یا از اپراتور تلفن همراه بابت تعادل پیش پرداخت شده کسر می‌گردد. با استفاده از پرداخت‌های مستقیم اپراتوری، کاربران تلفن همراه می‌توانند به راحتی و با سرعت بالا عملیات پرداخت به تجار، خرید کالاها یا خدمات واقعی یا مجازی و همچنین ایجاد سپرده یا ارسال پول را به انجام رسانند. از مزایای این روش می‌توان به سریع و آسان بودن، عدم نیاز به ارسال اطلاعات اکانت بانکی، عدم ارسال نام کاربری و رمزعبور و امن بودن به دلیل عدم ارسال هیچ یک از جزئیات شخصی، اشاره نمود. اما علی‌رغم این مزایا، اتصال مستقیم به پلتفرم صورت‌حساب اپراتور، نیازمند یکپارچگی با اپراتور است که این کار هزینه‌بر و وقت‌گیر می‌باشد.

پرداخت نوع دوم در حقیقت کیف پول تلفن همراه است که در شرایط ساده، یک سیستم پرداخت می‌باشد. تفاوت بین خدمات پرداخت آنلاین و کیف پول تلفن همراه، آن است که می‌توان از این کیف پول برای پرداخت در یک فروشگاه فیزیکی نیز استفاده کرد که بسیار ساده‌تر از کارت یا پول نقد است. این در حالی است که پرداخت‌های آنلاین تنها به منظور انجام پرداخت‌های مجازی قابل استفاده هستند. از مزایای این سیستم می‌توان به سهولت استفاده، در دسترس بودن، امکان هماهنگ‌سازی داده‌ها در دستگاه‌های مختلف تلفن همراه و عدم نیاز به همراه داشتن کارت بانکی اشاره نمود. برخی معایب این روش نیز، شامل اشکالات موجود در اتصال به شبکه‌های تلفن همراه، مشکلات هویتی در سرقت هویت افراد دارای کیف پول به دلیل ذخیره‌سازی اطلاعات کاربران در سطح تلفن همراه، نیاز به پیاده‌سازی زیرساخت مناسب و الزام به وجود تلفن همراه هوشمند در هنگام پرداخت، می‌باشد.

در پرداخت نوع سوم که پرداخت وب موبایل (WAP) نام دارد، مصرف‌کننده با استفاده از صفحات وب نمایش داده شده (IPG) یا برنامه‌های کاربردی که در تلفن همراه نصب شده‌اند، پرداخت را انجام می‌دهد. از مزایای این روش می‌توان به سریع و آسان بودن، قابل پیش‌بینی‌بودن و امکان انتقال داده‌ها به طور امن، اشاره نمود. اما از آنجا که در این روش، فقط ارتباط را می‌توانیم امن کنیم هنوز چالش‌های امنیتی سمت تلفن‌همراه از جمله حضور بدافزارها[2] و ثبت‌کننده‌های کلید[3] در این روش وجود دارد.

و پرداخت نوع چهارم، پرداخت مبتنی بر NFC می‌باشد. تکنولوژی NFC یک تکنیک ارتباطی بدون سیم و تکامل یافته‌تر از RFID است. فاصله‌ی عملکرد در این فناوری حدود ۴ اینچ است و در فرکانس ۱۳,۵۶ مگاهرتز با سرعت ۱۰۶، ۲۱۲ یا ۴۲۴ کیلوبیت بر ثانیه عمل می‌کند. استفاده از این تکنولوژی بدون در نظر گرفتن استانداردهایی که در سال‌های اخیر برای آن ارائه

[1] Direct Operator Billing
[2] malware
[3] key logger

شده است شامل آسیب‌پذیری‌هایی از جمله استراق سمع، دستکاری داده‌ها، خرابی داده، حملات کپی و فیشینگ است که منجر به نشت داده های حریم شخصی کاربران می شود. در صورت رعایت استانداردهای امنیتی مناسب و زیرساخت موجود در اپراتورهای همراه، می‌توان از این فناوری به عنوان زیرساخت سیستم پرداخت مؤثر و امن استفاده کرد. به این منظور مجموعه-ای از استانداردهای امنیت NFC تهیه شده است که عمده‌ی کار آن‌ها تسهیل در مدیریت کلید برای یک ارتباط امن می‌باشد [۱،۲].

تلفن‌های همراه محبوب‌ترین دستگاه‌های شخصی، فراگیر و در دسترس در هر مکانی هستند که به غیر از مکالمه و انتقال داده‌ها، ویژگی‌های اضافه‌ای مانند احراز هویت، تولید کلید و رمزنگاری را در خود، فراهم می‌کنند. پرداخت‌های موبایلی می‌توانند به کمک دستگاه تلفن همراه در هر زمان، در هر مکان و از هر نوعی که باشند، انجام پذیرند. از این رو بحث امنیت انتها به انتها برای پرداخت‌های تلفن همراه، بسیار حائز اهمیت می‌باشد. امنیت در سطح معاملات بایستی امنیت انتها به انتها، یکپارچگی، محرمانه بودن و عدم انکار پیام را تضمین کند. استفاده از کلیدهای عمومی (PKI) به منظور اطمینان از پایداری امنیت کلیه‌ی زیرساخت‌ها در تلفن‌های همراه مفید است اما از سوی دیگر، کلیدهای مخفی ذخیره‌شده در حافظه‌ی تلفن همراه، موجب نگرانی‌های جدیدی از جمله آلوده شدن کلیدها توسط ویروس و یا جایگزین شدن آن‌ها به صورت مخرب، شده است [۳].

در توافقنامه کلیدی، هر موجودیت در اکوسیستم پرداخت باید مدارک خود را برای به دست آوردن کلید عمومی با دیگر موجودیت‌ها، مبادله کند. به طور خاص، گواهینامه، شامل اطلاعات شخصی کاربر است. بنابراین، مهاجم می تواند با ردیابی رفتار کاربر ، حریم خصوصی او را به خطر بیاندازد. پروتکل حفاظت از حریم خصوصی مبتنی بر NFC، از مؤلفه TSM در نقش یک شخص ثالث مورد اعتماد در فرایند ثبت نام کاربر، استفاده کرده و در صورت لزوم هویت طرفین را تأیید می کند [4].

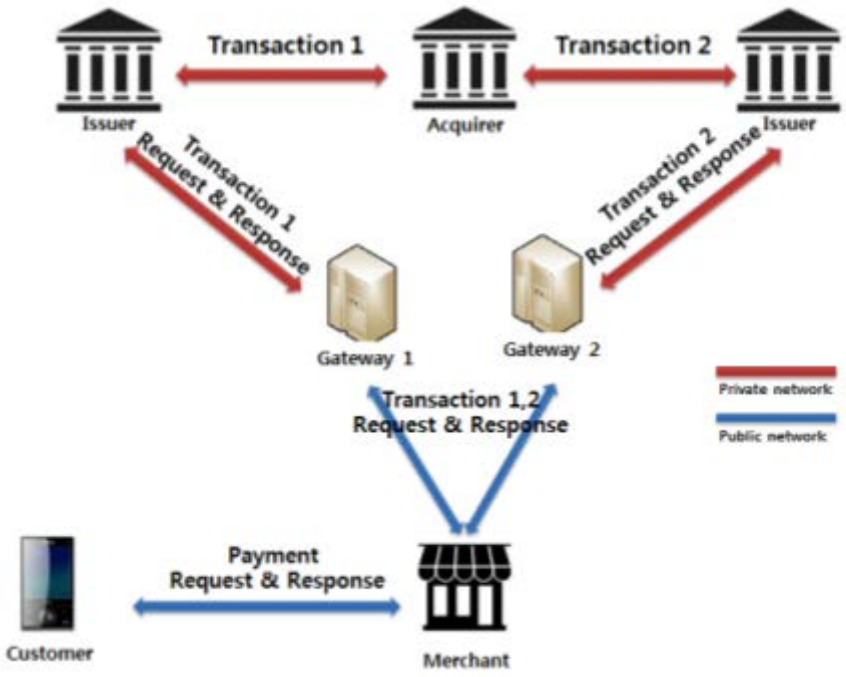
همانطور که بیان شد، در هیچ‌یک از روش‌های پرداخت، نیاز به حمل‌و نقل کارت اعتباری وجود ندارد. این امر استفاده از مفهوم کارت مجازی برای انجام تراکنش‌های بانکی را توجیه می‌کند. لذا در مقاله حاضر به ارائه‌ی یک قاب‌کاری برای پرداخت امن در تلفن همراه مبتنی بر سیم‌کارت (USIM) که تنها مؤلفه‌ی مورد اعتماد در دستگاه تلفن همراه است می‌پردازیم.

۲- ادبیات موضوع

همانطور که در بخش پیش اشاره شد، یکی از چالش‌های اساسی در حوزه‌ی پرداخت، جعل هویت کاربران و مخفی نبودن اطلاعات آنها می‌باشد. مراجع [۴،۱۰] به امکان‌سنجی پیاده‌سازی یک اکوسیستم پرداختی با استفاده از عنصر امن (SE)، پرداخته‌اند. این پژوهش، ابتدا به بیان انواع معماری‌های عنصر امن یعنی SIM-centric، device-centric ، Host Card و Emulation پرداخته و از بیان معماری‌هایی نظیر SD-centric که در صنعت رایج نیست صرف نظر کرده است. همچنین چارچوب‌های چندجانبه‌ای برای پلت‌فرم پرداخت موبایلی ارائه کرده است که از سه لایه‌ی ارائه دهنده (شامل شرکت‌های تولیدکننده تلفن همراه، اپراتورهای تلفن همراه، شرکت‌های ارائه دهنده کارت‌های اعتباری، بانک‌ها و مانند آن)، لایه‌ی تکنولوژی (شامل پلت‌فرم پرداخت موبایلی) و لایه‌ی کاربر (شامل مردم و تاجران)، تشکیل شده است. این مرجع در نهایت به تجزیه و تحلیل استراتژیک اکوسیستم پرداخت تلفن با بررسی رابطه بین معماری SE و پلت‌فرم‌های پرداختی موجود، پرداخته است.

در مرجع [۵]، پیشنهاد یک طرح پرداخت سبک وزن بر اساس دو دروازه ارائه شده است. این مرجع نشان می‌دهد که طرح

پیشنهادی، الزامات امنیتی ضروری مانند پاسخگویی و اطمینان را تضمین می‌کند. طرح پیشنهادی دارای چهار شرکت کننده شامل مشتری، بازرگان و دو دروازه‌ی پرداخت می‌باشد که در شکل ۱ نشان داده شده است. همچنین یک شبکه امن داخلی، بین دو صادر کننده، خریدار و دو دروازه فرض شده است.



شکل ۱. مکانیزم پرداخت موبایل بر اساس دو درگاه [۵]

در مرجع [۶]، با استفاده از تکنولوژی NFC و معماری شبکه GSM، یک سیستم پرداخت خرد[4] برای تلفن همراه ارائه شده است. این نوع پرداخت، قشر گسترده‌ای از پرداخت‌های موبایلی را پوشش می‌دهد. البته شایان ذکر است که این نوع پرداخت‌ها می‌توانند از نوع پرداخت فرد به فرد باشند و در انتقالات تجاری تجار جایی ندارد. احراز هویت در این سیستم از طریق سیم-کارت و رمزنگاری داده‌های ارسالی از طریق رمزنگاری لایه‌ی GSM صورت می‌پذیرد. این مسئله، ادغام این سیستم با شبکه زیرساخت تلفن همراه را آسان می‌کند. استفاده از NFC برای ارتباطات کوتاه برد با دستگاه‌های POS[5] به جای کارت‌های بانکی باعث شده که از دیدگاه مشتری و بازرگانان، روند پرداخت بدون تغییر باقی بماند. در روش ارائه شده در مرجع مذکور، امنیت برای پرداخت‌های کم ارزش، قابل قبول است.

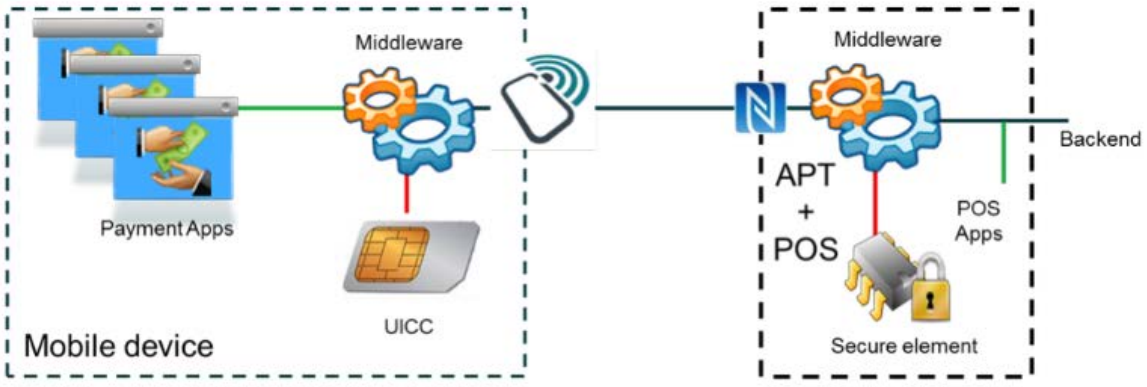
مرجع [۷]، سیستم‌های پرداخت موبایلی را در پنج دسته شامل استفاده از تلفن همراه در دستگاه‌های POS، استفاده از دستگاه تلفن همراه به عنوان دستگاه POS، پلت‌فرم پرداخت موبایلی، سیستم پرداخت موبایلی مستقل و صورت‌حساب مستقیم اپراتور تفکیک می‌نماید. در این مقاله، خدمات امنیتی موردنظر در سیستم‌های پرداخت تلفن همراه و همچنین مکانیزم‌های امنیتی که در حال حاضر در آن قرار دارد، به طور خلاصه بیان شده است و به سه تهدید امنیتی، یعنی بدافزار،

[4] micro payment
[5] Point-of-Sale

آسیب‌پذیری‌های SSL/TLS و نقض داده‌ها و نیز چهار چالش امنیتی شامل شناسایی بدافزار، احراز هویت چند عامله، جلوگیری از نقض اطلاعات، و تشخیص و جلوگیری از تقلب در پرداخت تلفن همراه، پرداخته است.

در مرجع [۸]، ادعا شده است که تعداد زیادی از مطالعات راجع به سیستم‌های پرداخت تلفن همراه در سال های اخیر صورت گرفته است که طرح‌های ارائه شده عمدتا بر روی امنیت مبادلات تمرکز می‌کنند نه در زمینه حفظ و حراست از حریم خصوصی کاربران. در این مقاله یک طرح پرداخت ناشناس غیرقابل پیگیری، برای ارائه محیط امن پیشنهاد شده است که کاربر می‌تواند یک کارت اعتباری مجازی و ناشناس را از یک مدیر سرویس معتبر (TSM) درخواست کند. اطلاعات حساس کارت اعتباری اعمال شده در عنصر امن دستگاه تلفن همراه کاربر ذخیره می‌شود. پروتکل پیشنهادی ویژگی‌های مختلف امنیتی مهمی نظیر نامعلوم بودن، قطع ارتباط و عدم نفوذ پذیری و غیره را تضمین می‌کند.

در مرجع [۹]، یک راه حل سرویس تلفیقی یکپارچه مبتنی برNFC ارائه شده است که تحت پروژه تحقیقاتی MobiPag توسعه یافته است. یکی از مشخص‌ترین ویژگی‌های Mobipag، مدل معماری باز آن است که به شرکای متعدد اجازه می‌دهد تا بخشی از زنجیره ارزش سیستم پرداختی شوند و راه‌حل‌هایی را ایجاد کنند که پرداخت ها را به روش‌های غیر منتظره ای انجام دهند. بر اساس نتایج این آزمایش، تعدادی از چالش‌ها و دستورالعمل‌ها شناسایی شده و استفاده از آن‌ها در سیستم‌های پرداخت مبتنی بر NFC آینده، امکان‌پذیر می‌باشد. همانطور که در شکل ۲ مشاهده می‌شود، این مقاله ارتباط بین یک تلفن همراه و دستگاه POS را به تفصیل توضیح داده و بیان نموده که هر بخش از این ارتباط، توسط کدام عنصر انجام می‌پذیرد.



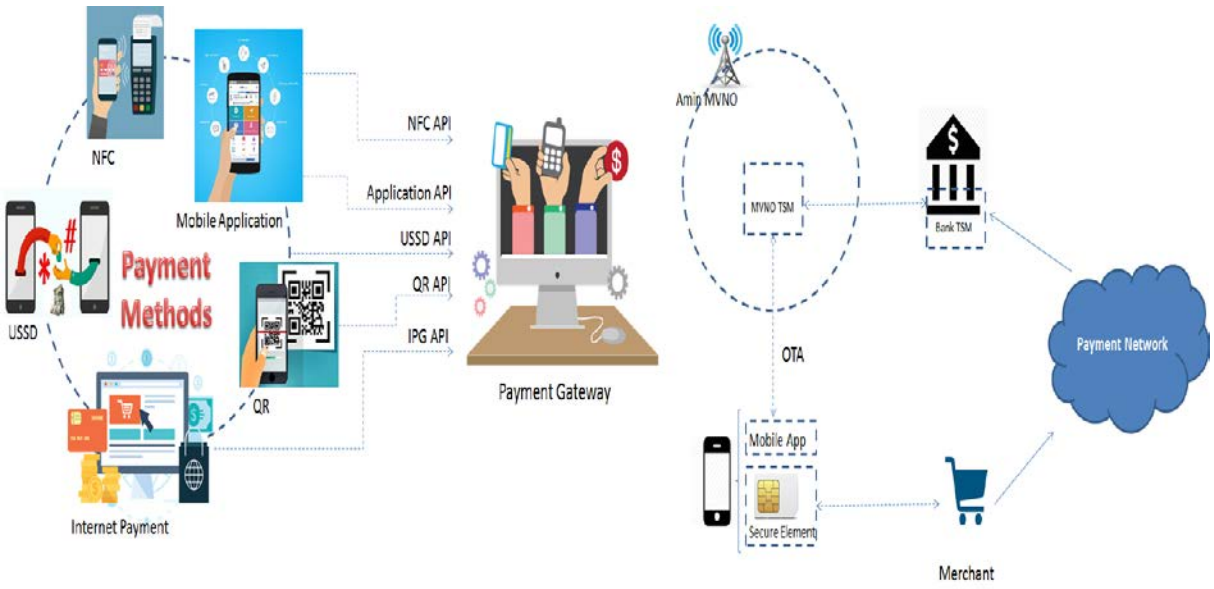
شکل.۲ معماری تلفن‌همراه و دستگاه POS [۹]

۳- معماری سامانه جامع پرداخت پیشنهادی

در این مقاله به ارائهٔ یک بستر جامع و امن برای پرداخت‌های موبایلی، مبتنی بر سیم‌کارت، می‌پردازیم. تغییر در زیرساخت‌های مخابراتی برای ایمن‌سازی پروتکل‌های موجود، کاری غیر ممکن است لذا با توجه به تنوع در روش‌های پرداخت موبایلی از جمله USSD، NFC، BLE، کدهایQR، RFID و موبایل اپلیکیشن‌ها لازم است ضمن بررسی سطح حمله‌ی هر کدام از این روش‌ها، یک روش جامع پرداخت با لحاظ کردن مسائل امنیتی، حفظ سادگی و با استفاده از یک مدل اعتماد مبتنی بر سیم-

کارت ارائه گردد.

طرح پیشنهاد شده در این مقاله، یک زیرساخت امن یکپارچه بر روی بستر مخابرات سیار است که دارای سه مؤلفه اصلی شامل کاربرد نصب شده بر روی سیم‌کارت به منظور رمزنگاری و مدیریت کلیدها، درگاه امن در سمت اپراتورها به منظور تطبیق پروتکل‌ها و یک هماهنگ‌کننده کارگزار قراردادهای تجاری بین اپراتورهای شبکه تلفن همراه، بانک‌ها و ارائه‌دهندگان خدمات پرداختی (TSM) می‌باشد. شکل ۳ معماری مفهومی زیرساخت امن پرداخت پیشنهادی را به تصویر می‌کشد. برای استفاده هر کاربر از این زیرساخت، نیاز به طی دو فاز شامل تولید کلیدهای اشتراکی و تولید کارت اعتباری مجازی می‌باشد. این دو فاز در ادامه شرح داده می‌شود.



شکل ۳. معماری مفهومی سامانه جامع پرداخت

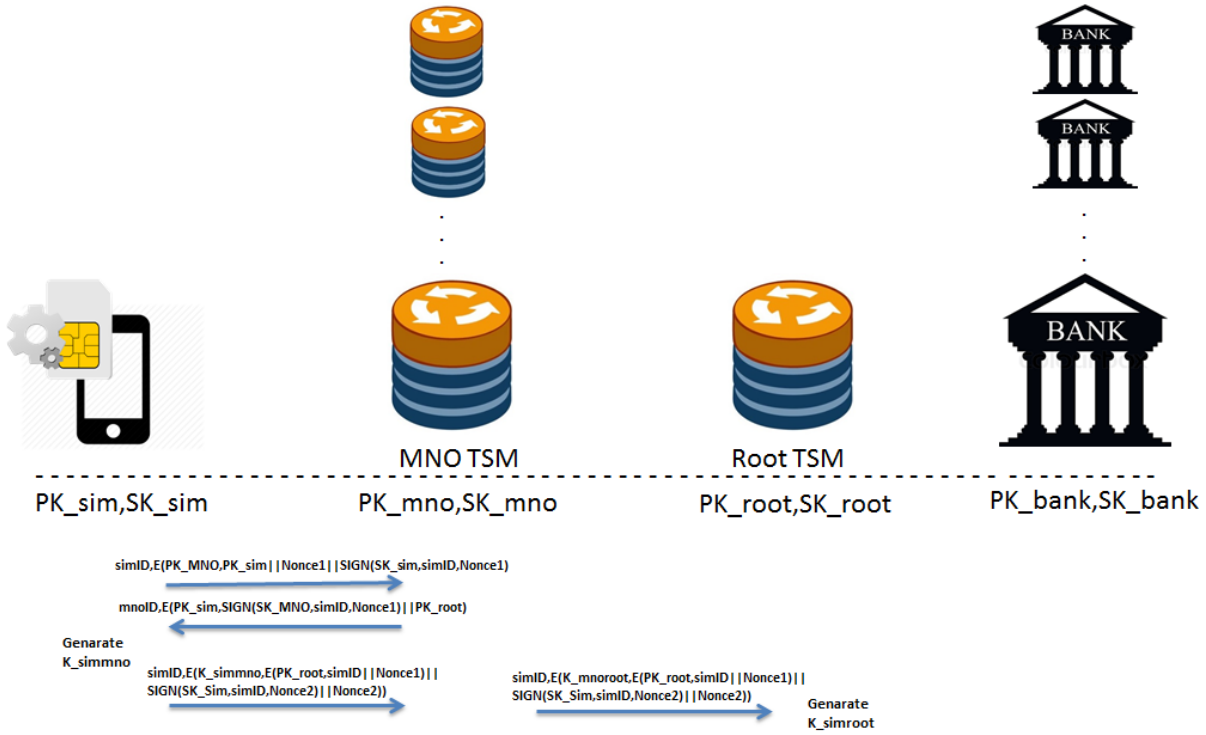
۳-۱- فاز تولید کلیدهای اشتراکی

مطابق شکل ۴، موجودیت‌های این سامانه شامل بانک، سامانه مورد اعتماد مربوط به اپراتور تلفن همراه (MNO TSM)، سامانه مورد اعتماد مرکزی (ROOT TSM)، و سیم‌کارت می‌باشند. با فرض اینکه بین هریک از موجودیت‌ها غیر از کاربر، کلیدهای اشتراکی برای تبادل امن اطلاعات وجود دارد، در این بخش بین هر یک از موجودیت‌ها و کاربر، به منظور برقراری ارتباط امن، کلید اشتراکی می‌سازیم. مراحل این عملیات به شرح زیر می‌باشد:

- **مرحله ۱:** ابتدا کاربر کلید عمومی متناظر با master key سیم‌کارت خود را تولید نموده و آن را با استفاده از کلید خصوصی خود امضا و با کلید عمومی اپراتور رمز نموده و برای اپراتور به عنوان درخواست اولیه ارسال می‌نماید.
- **مرحله ۲:** اپراتور پس از رمزگشایی بستهٔ دریافتی توسط کلیدهای خصوصی خود، کلید عمومی کاربر را استخراج نموده و بر اساس آن یک کلید اشتراکی تولید نموده و آن را درون بسته‌ای امن که با کلید خصوصی خود امضا شده

برای سیم‌کارت، از بستر مخابرات ارسال می‌نماید.

- **مرحله ۳:** سیم‌کارت با استفاده از کلید خصوصی خود بسته را رمزگشایی نموده و کلید اشتراکی بین خود و اپراتور را از آن استخراج نموده و در بخش خصوصی سیم‌کارت ذخیره می‌نماید.
- **مرحله ۴:** کاربر درخواست تولید کلید اشتراکی با ROOT TSM را به اپراتور ارسال می‌نماید و اطلاعاتی همچون شناسه خود را با کلید خصوصی خود امضا و با استفاده از کلید اشتراکی بین خود و اپراتور رمز می‌کند.
- **مرحله ۵:** در این مرحله اپراتور پس از بررسی درخواست و رمز کردن بسته دریافتی از کاربر، آن را مستقیما برای ROOT TSM ارسال می‌کند. همچنین مثل همه‌ی مراحل، بسته ارسالی باید با کلید خصوصی MNO TSM امضا شده باشد.
- **مرحله ۶:** ROOT TSM پس از رمزگشایی بسته با استفاده از کلید خصوصی خود، کلید اشتراکی بین خود و کاربر را استخراج می‌کند.



شکل۴. مراحل مربوط به کلید اشتراکی بین کاربر و بانک

۳-۲- فاز تولید کارت مجازی

در فاز قبل به تولید کلیدهای اشتراکی بین کاربر و همه‌ی موجودیت‌های دیگر سیستم پرداختیم. در این فاز قصد داریم که با استفده از کلیدهای موجود، اطلاعات مربوط به حساب‌های بانکی که در نظر داریم تا برای آنها کارت مجازی تولید کنیم را

برای بانک ارسال نماییم. مراحل این عملیات مطابق شکل ۵ به شرح زیر می‌باشد:

- **مرحله ۱:** در این مرحله کاربر با استفاده از کلیدهایی اشتراکی بین خود و بانک (که توسط هیچ یک از موجودیت‌های دیگر قابل رمزگشایی نیست) اطلاعات مربوط به کارت و رمزدوم خود را رمز و با استفاده از کلید خصوصی سیم‌کارت آن را امضا نموده و برای MNO TSM ارسال می‌نماید.

- **مرحله ۲:** همانند مرحله قبل اپراتور بسته دریافتی را بدون هیچ اعمالی با استفاده از کلیدهای اشتراکی رمز و با استفاده از کلید خصوصی خود امضا نموده و برای ROOT TSM ارسال می‌نماید.

- **مرحله ۳:** ROOT TSM، پس از رمزگشایی اطلاعات مربوط به حساب را به منظور احراز هویت سمت بانک ارسال می‌نماید (قابل ذکر است که بین ROOT TSM و بانک نیز کلیدهای اشتراکی وجود دارد که با استفاده از آنها داده‌ها در بستری امن تبادل می شوند)

- **مرحله ۴:** در این مرحله بانک پس از احراز هویت و تطابق اطلاعات بانکی کاربر، در صورت تایید شدن اطلاعات بانکی برای آن کاربر کارت مجازی مطابق با استانداردهای EMV، تولید می‌کند و آن را با استفاده از کلیدهای اشتراکی برای ROOT TSM ارسال می‌نماید.

- **مرحله ۵:** ROOT TSM اطلاعات مربوط به کارت مجازی را در بستری امن و به همراه امضا ی خود بر اپراتور ارسال می‌نماید.

- **مرحله ۶:** اپراتور نیز بسته مربوطه را که شامل اطلاعات مربوط به کارت مجازی در بستری امن و روی بستر مخابرات سیار برای کاربر ارسال می‌نماید.

- **مرحله ۷:** کاربر پس از دریافت بسته رمزشده، آن را رمزگشایی نموده و اطلاعات کارت بانکی مجازی را درون ماژول امن سیم‌کارت ذخیره‌سازی می‌کند و از این پس در پرداخت‌های مبتنی بر NFC، برنامه‌های کاربردی موبایل و پرداخت‌های USSD و مانند آن، از این کارت مجازی استفاده می‌کند.

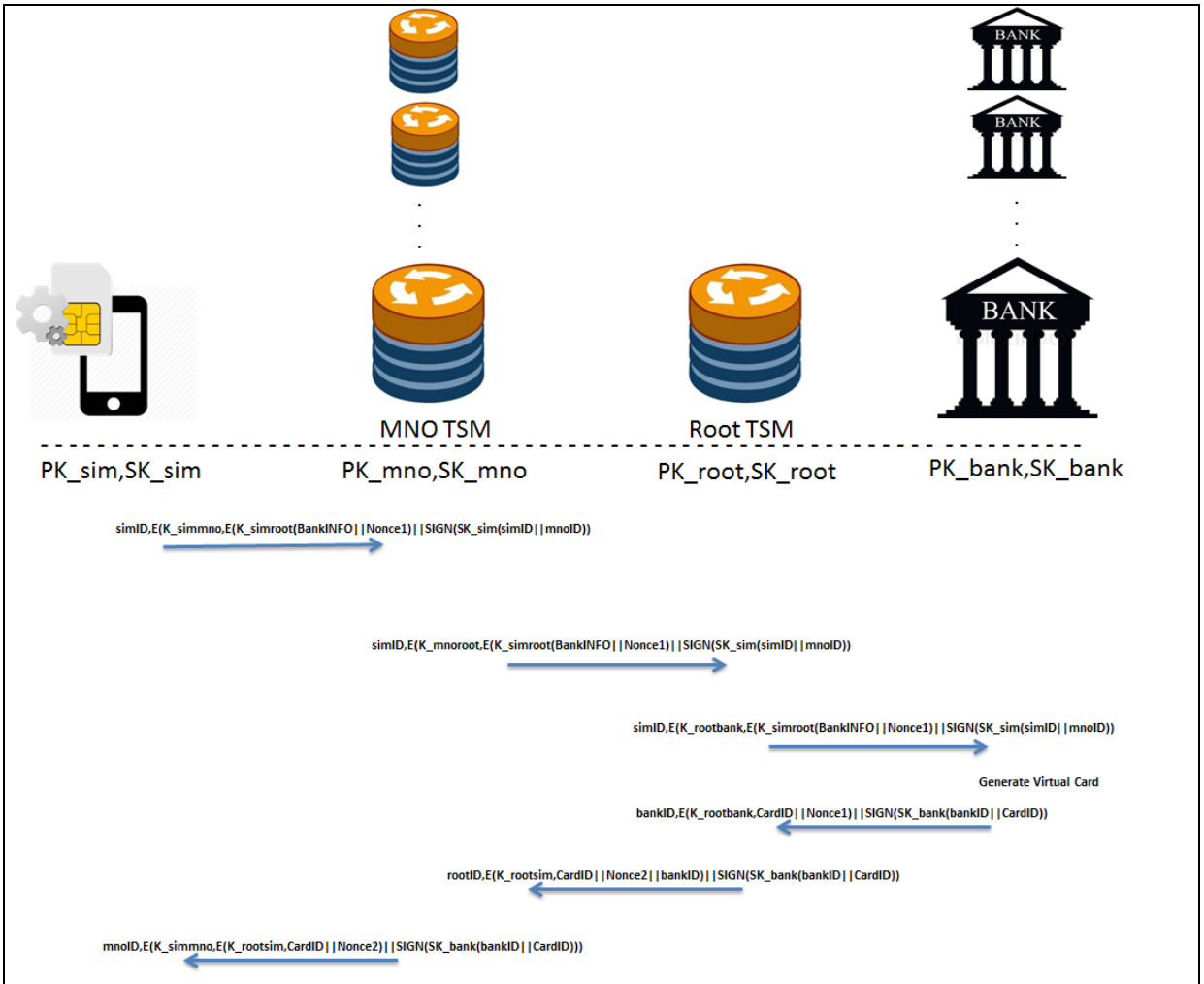
۴- یافته‌ها و نتایج

در این مقاله به بررسی روش‌های مختلف پرداخت و چالش‌های مختلف در هریک از این روش‌ها پرداخته و به ارائهٔ یک زیرساخت پرداخت جامع و امن مبتنی بر استانداردهای NFC اقدام نمودیم. در ادامه مشکلات و چالش‌های امنیتی که براساس این روش حل شده است را بیان می‌نماییم.

- **محرمانگی:** از آنجا که اطلاعات مربوط به حساب بانکی و احراز هویت آنها توسط پیام‌های که بین کاربر و بانک تبادل می شود توسط کلیدهای نامتقارن و اشتراکی رمزنگاری می‌شوند، هیچ کدام از موجودیت‌های بین راه و هرکس دیگر توانایی رمزگشایی آن را ندارد. همانطور که روشن است کلیدهای توافق شده در بانک در HSM بانک قرار می‌گیرد و در سمت کاربر کلیدها در ماژول امن سیم‌کارت قرار می‌گیرد که فقط با مجوزهای خاص می‌توان به

آن دسترسی داشت.

- **جامعیت:** به طور کلی، در بحث امنیت اطلاعات، منظور از جامعیت پیام این است که نسبت به عدم تغییر داده‌ها تضمین وجود داشته باشد و یا به عبارت دیگر، هیچ کس قادر به ویرایش، دستکاری و یا تخریب داده‌ها نباشد.
- در معماری راهکار حاضر، اگر یک مهاجم، پیام ارسالی از سوی کاربر را تغییر دهد، امکان وقوع این حمله غیرممکن است. زیرا هنگامی که بانک یا هر یک از موجودیت‌های بین راه پیام را دریافت می‌کند با بررسی امضای بسته ارسالی و مقایسه آن هرگونه تغییر و دستکاری در بسته قابل تشخیص است. و بدین ترتیب از عدم دستکاری و یا تخریب پیام دریافتی اطمینان حاصل می‌شود.
- **ناشناس:** در طول درخواست کاربران برای یک کارت بانکی مجازی، احراز هویت متقابل تنها با بانک انجام می شود. بنابراین، تنها بانک هویت واقعی کاربران را می‌داند. وقتی کاربران از کارت مجازی خود برای درخواست معامله ناشناس از TSM استفاده می‌کند، TSM هویت کاربر را نمی داند و همچنین بازرگانان هویت کاربر را نیز نمی‌دانند.
- **عدم ارتباط:** همانطور که در طرح ارائه شد بیان، موجودیت مورد اعتماد در سمت اپراتور و بانک متفاوت است. در واقع سامانه مورد اعتماد سمت اپراتور با استفاده از کلیدهای اشتراکی خود با کاربر از بستر OTA روی سیم‌کارتها داده بارگذاری می‌کنند که این امر نیاز به اطلاعاتی دارد که فقط در اختیار اپراتور است و نباید بانک ار آن‌ها با خبر باشد و همچنین اطلاعاتی که TSM مربوط به اپراتور منتقل می‌کند یک کارت مجازی است و محرمانگی اطلاعات مربوط به کارت بانکی در این بخش به خطر نمی‌افتد. از سوی دیگر سامانه مورد اعتماد بانک‌ها با استفاده ز کلیدها و مجوزهای اشتراکی بین خود و بانک می‌توانند عملیاتی مربوط به کارت بانکی و ژداخت‌ها را ئیگیری کنند و نیاز به اطلاعات محرمانه اپراتورها وجود ندارد. و بین کاربر و بانک کارت بانکی مجازی وجود دارد که برای هیچ یک از موجودیت‌ها قابل دسترسی نیست، بنابراین ارتباط ببین کاربر و بانک از دیدگاه بازرگانان و ارائه دهندگان خدماتت، کاملا ناشناس می‌ماتد
- **عدم انکار:** از آنجا که اطلاعات تبادل شده بین موجودیت‌ها در هر مرحله با استفاده از کلید خصوصی خود آن موجودیت رمز می شود، پس هیچ کاربر و یا هیچ سامانه مورد اعتماد سوم شخصی که در این طرح ارائه شئه نمی‌تواند پیام ارسالی خود را انکار کند.
- **جلوگیری از حمله بازپخش یا تکرار:** از آنجا که در طرح ارائه شده، هر پیام با یک nonce رمزگذاری می شود. با تغییر مقادیر تصادفی در هر جلسه، مهاجمان نمی توانند پیام های قبلی را برای تصدیق هویت ما ارسال کنند. در حقیقت، بی فایده است که مهاجمان پیام هایی را که کاربر برای درخواست یک کارت مجازی درخواست می کنند پخش کند، زیرا پیام ها همه رمزگذاری شده اند و مقدار تصادفی ای دارند که پس از یک بار استفاده و یا بعد از زمان کوتاهی منقضی می شود.



شکل۵. مراحل مربوط به ساخت کارت بانکی مجازی

فهرست مراجع

[1] Ling, J., Wang, Y., & Chen, W. (2017). An improved privacy protection security protocol based on NFC. International Journal Network Security, 19, 39-46.

[2] Ondrus, J. (2015, August). Clashing over the NFC Secure Element for Platform Leadership in the Mobile Payment Ecosystem. In Proceedings of the 17th International Conference on Electronic Commerce 2015 (p. 30). ACM.

[3] Ahamad, S. S., Sastry, V. N., & Udgata, S. K. (2014). Secure mobile payment framework based on UICC with formal verification. International Journal of Computational Science and Engineering, 9(4), 355-370.

[4] Ondrus, J. (2015, August). Clashing over the NFC Secure Element for Platform Leadership in the Mobile Payment Ecosystem. In Proceedings of the 17th International Conference on Electronic Commerce 2015 (p. 30). ACM

[5] Lee, H., Kim, J., Moon, J., Kang, D., & Won, D. (2017). A Security Enhanced Lightweight Mobile Payment Scheme Based on Two Gateways. biometrics, 3, 9.

[6] Chen, W., Hancke, G. P., Mayes, K. E., Lien, Y., & Chiu, J. H. (2010, April). NFC mobile transactions and authentication based on GSM network. In Near Field Communication (NFC), 2010 Second International Workshop on (pp. 83-89). IEEE.

[7] Wang, Y., Hahn, C., & Sutrave, K. (2016, February). Mobile payment security, threats, and challenges. In Mobile and Secure Services (MobiSecServ), 2016 Second International Conference on (pp. 1-5). IEEE.

[8] Luo, J. N., Yang, M. H., & Huang, S. Y. (2016). An Unlinkable Anonymous Payment Scheme based on near field communication. Computers & Electrical Engineering, 49, 198-206.

[9] Rodrigues, H., José, R., Coelho, A., Melro, A., Ferreira, M. C., Monteiro, M. P., & Ribeiro, C. (2014). MobiPag: Integrated Mobile Payment, Ticketing and Couponing Solution Based on NFC. Sensors, 14(8), 13389-13415.

[10] de Reuver, M., & Ondrus, J. (2017). When Technological Superiority is not Enough: The Struggle to Impose the SIM Card as the NFC Secure Element for mobile payment platforms. Telecommunications Policy, 41(4), 253-262.

[11] https://www.mobiletransaction.org/different-types-of-mobile-payments/