

الحمد لله
الرحمن
الرحيم



دانشگاه قم

دانشکده فنی مهندسی

پایان نامه کارشناسی ارشد رشته فناوری اطلاعات گرایش تجارت الکترونیک

عنوان:

مقایسه روش‌های امنیتی برای افزایش اطمینان

در پرداخت سیار با استفاده

از تکنولوژی ارتباط میدان نزدیک NFC

استاد راهنما:

دکتر فرانک فتوحی قزوینی

استاد مشاور:

دکتر یعقوب فرجامی

نگارنده:

غدیر صفاء مجید

شهریور / ۱۳۹۳

تقدیم به:

آستان حقیقت

و آنان که وصالش را می جویند،
آنان که در آغوشش کشیده‌اند و
آنان که خود، عین حقیقت‌اند

تشکر و قدردانی

حمد و سپاس خدای را که توفیق کسب دانش و معرفت را به ما عطا فرمود. در اینجا بر خود لازم می‌دانم از تمامی اساتید بزرگوار، به‌ویژه اساتید دوره کارشناسی ارشد که در طول سالیان گذشته مرا در تحصیل علم و معرفت و فضائل اخلاقی یاری نموده‌اند تقدیر و تشکر نمایم. از استاد گرامی و بزرگوار سرکار خانم دکتر فرانک فتوحی قزوینی که راهنمایی این‌جانب را در انجام تحقیق، پژوهش و نگارش این پایان‌نامه تقبل نموده‌اند نهایت تشکر و سپاسگزاری را دارم. همچنین از اساتید محترم جناب آقای دکتر یعقوب فرجامی، به‌عنوان استاد راهنمای دوم به خاطر راهنمایی‌های ارزنده، مساعدت‌ها و دلسوزی‌هایشان در طول انجام این پژوهش کمال تشکر را دارم. از اعماق قلبم سپاسگزار خانواده‌ام هستم که همواره پشتیبان من بودند و از انجام هیچ کاری برای کمک به من فروگذار نبودند.

چکیده:

با افزایش نفوذ تلفن همراه و توسعه تجارت سیار، استفاده از تلفن همراه به عنوان ابزار پرداخت روزبه روز گسترش می یابد. به دلیل اهمیت امنیت در تجارت و پرداخت و نیز ویژگی های منحصر به فرد شبکه های بی سیم و محدودیت های موجود در ابزار پرداخت، پروتکل های پیشنهادی در حوزه پرداخت سیار علاوه بر تأمین کارایی می بایستی از امنیت مناسبی نیز برخوردار باشند. ارتباط میدان نزدیک (NFC)، ارتباط غیر تماسی را در تعامل دستگاه های تلفن همراه نزدیک به هم از طریق یک کانال بی سیم را ایجاد می کند. تکنولوژی آن، با استانداردهای کارت هوشمند موجود، سازگار است.

مصونیت اطلاعات در پرداخت امری حیاتی است. استراق سمع یکی از بیشترین حملاتی است که فن آوری های مختلفی همچون کیف پول گوگل، NFC و دستگاه شناسایی فرکانس رادیویی (RFID) را مورد هدف قرار می دهد. محققان و کارشناسان امنیتی مکانیسم های مختلف دفاعی، برای حفاظت داده های خصوصی در مقابل دسترسی های غیرمجاز را طراحی کرده اند.

این پایان نامه یک لایه ای امنیتی را، با ادغام دو نوع مکانیسم دفاعی شناخته شده اضافه می کند، برای جلوگیری حمله بین دو دستگاه ارتباطی در حالت فعالیت مناسب است. این پروتکل ها برای انجام پرداخت ایمن به کار می روند. اولی با استفاده از الگوریتم رمزنگاری متقارن و پنهان نگاری کار می کند و پروتکل دیگر با استفاده از الگوریتم رمزنگاری کلید عمومی و امضای دیجیتال مکانیسم دفاعی را ایجاد می کند. پروتکل ادغامی توسط برنامه نویسی اندروید برای دستگاه تلفن همراه پیاده سازی شد. این پروتکل به صورت یک لایه امنیتی در دو برنامه مجزای مشتری و تاجر در یک سیستم پرداخت به کار گرفته شده است.

کلمات کلیدی: سیستم پرداخت سیار، ارتباط میدان نزدیک (NFC)، امنیت، حالت نظیر به نظیر،

تلفن همراه، برنامه نویسی اندروید

فهرست مطالب

۱	فصل اول: کلیات پژوهش
۲	۱-۱ مقدمه
۳	۲-۱ ضرورت پژوهش
۳	۳-۱ اهداف و سؤالات پژوهش
۴	۴-۱ جنبه جدید بودن و نوآوری پژوهش
۴	۵-۱ روش پژوهش
۵	۶-۱ ساختار پژوهش
۶	۷-۱ چکیده فصل
۷	فصل دوم: مرور ادبیات تحقیق و کارهای مرتبط
۸	۱-۲ مقدمه
۸	۲-۲ سیستم‌های پرداخت و انواع آن
۹	۱-۲-۲ کارت نوار مغناطیسی
۹	۱-۲-۲-۱ امنیت در کارت نوار مغناطیسی
۹	۲-۲-۲ کارت‌های هوشمند (گروه‌بندی بر اساس مکانیزم)
۱۰	۱-۲-۲-۲ کارت‌های هوشمند تماسی
۱۱	۲-۲-۲-۲ کارت‌های هوشمند غیرتماسی
۱۲	۳-۲-۲-۲ مدل‌های ترکیبی
۱۲	۴-۲-۲-۲ امنیت در کارت هوشمند
۱۹	۳-۲ پرداخت سیار
۱۹	۱-۳-۲ تکنولوژی NFC
۲۰	۱-۳-۲ استانداردها و پروتکل‌های مرتبط با NFC
۲۵	۲-۳-۲ دستگاه‌های هوشمند دارای تکنولوژی NFC
۲۷	۳-۳-۲ حالت عملیاتی NFC
۳۲	۴-۳-۲ برنامه‌های کاربردی NFC
۳۵	۵-۳-۲ معماری موبایل‌های NFC و اجزای اصلی آن
۴۶	۲-۳-۲ فناوری امنیت NFC

۴۷ NFC روش احراز هویت
۴۷ فاز ثبت نام
۴۸ فاز احراز هویت
۵۰ آنالیز و تحلیل
۵۰ تجزیه و تحلیل امنیت
۵۱ تجزیه و تحلیل کارآمد
۵۲ عناصر امنیت در معماری NFC
۵۳ عملیات کنترل امنیت/ مالکیت و شخصی سازی
۵۴ نصب اولیه، شخصی سازی و مدیریت
۵۵ مهاجرت
۵۷ سوء استفاده کردن از تلفن های همراه NFC
۵۹ تهدیدات
۵۹ استراق سمع
۶۱ انحراف داده
۶۱ تغییر داده
۶۳ الحاق داده
۶۳ حمله فرد مداخله گر
۶۵ حمله کلاه برداری URI پوسترهای هوشمند و مرورگر وب
۶۶ انکار سرویس (دستگاه)
۶۶ حمله انکار سرویس (المان امنیت)
۶۷ تگ های شبیه سازی
۶۸ حمله بازپخش و سرقت اطلاعات
۶۹ تکه تکه کردن پشته NFC اندروید
۷۱ کانال امن برای NFC
۷۱ قرارداد کلید ویژه NFC
۷۴ مروری بر کارهای مرتبط
۷۷ خلاصه فصل
۷۸ فصل سوم: الگوریتم های استفاده شده در پژوهش
۷۹ مقدمه
۷۹ الگوریتم های رمزنگاری
۸۲ الگوریتم رمزنگاری متقارن
۸۲ رمزنگاری با استاندارد رمزنگاری پیشرفته
۸۵ الگوریتم رمزنگاری نامتقارن
۸۶ رمزنگاری نامتقارن با امضای دیجیتالی

۸۷	مقایسه الگوریتم‌های رمزنگاری متقارن و نامتقارن
۸۸	پنهان‌نگاری
۹۱	پیاده‌سازی در اندروید
۹۳	امنیت اندروید
۹۴	مشکلات امنیتی برنامه‌های موبایل
۹۷	۳-۳ چکیده فصل
۹۸	فصل چهارم: الگوریتم‌های پیشنهادی
۹۹	۱-۴ مقدمه
۱۰۰	۲-۴ پروتکل پیشنهادی چند لایه‌ای امنیتی با الگوریتم رمزنگاری AES و پنهان‌نگاری
۱۰۰	۱-۲-۴ معماری سیستم الگوریتم امنیتی چند لایه‌ای
۱۰۰	۲-۲-۴ طراحی سیستم
۱۰۰	۳-۲-۴ توصیف ساختاری سیستم
۱۰۱	۴-۲-۴ کانال ایمن
۱۰۲	۵-۲-۴ منبع کلید ۱۲۸ AES
۱۰۲	۶-۲-۴ تبادل کلید
۱۰۲	۳-۴ پروتکل پیشنهادی پرداخت با استفاده از رمزنگاری نامتقارن همراه با امضای دیجیتال
۱۰۳	۱-۳-۴ معماری سیستم
۱۰۳	۲-۳-۴ طراحی سیستم
۱۰۳	۳-۳-۴ توصیف ساختاری سیستم
۱۰۴	۱-۳-۳-۴ پروتکل پرداخت خرد غیر برخط
۱۰۶	۲-۳-۳-۴ پروتکل پرداخت خرد برخط
۱۰۷	۴-۴ پیاده‌سازی برنامه مشتری و تاجر در اندروید
۱۰۸	۱-۴-۴ NFC در اندروید
۱۰۸	۱-۱-۴-۴ API های اندروید در NFC
۱۰۹	۲-۱-۴-۴ سیستم ارسال اینترنت تگ و سیستم ارسال در پیش زمینه
۱۱۰	۳-۱-۴-۴ ارسال تگ NFC به برنامه
۱۱۱	۴-۱-۴-۴ دریافت تگ با فرمت NDEF در اندروید
۱۱۲	۵-۱-۴-۴ ویژگیهای NFC در فایل منیفست اندروید
۱۱۳	۶-۱-۴-۴ اینترنت فیلتر در NFC
۱۱۷	۷-۱-۴-۴ چک کردن آدابتور NFC
۱۱۷	۸-۱-۴-۴ آماده کردن داده NDEF
۱۱۹	۹-۱-۴-۴ دریافت پیام NDEF
۱۲۰	۱۰-۱-۴-۴ پردازش پیام NDEF

۱۲۱ ۱۱-۱-۴-۴ رکورد برنامه اندروید
۱۲۲ Peer-to-Peer در حالت NFC برنامه ۱۲-۱-۴-۴
۱۲۴ NDEF پیام‌های ۱۳-۱-۴-۴
۱۲۵ setNdefPushMessage() استفاده از متد ۱۴-۱-۴-۴
۱۲۶ دریافت بیم ۱۵-۱-۴-۴
۱۲۹ AES پیاده‌سازی در اندروید ۲-۴-۴
۱۲۹ AES API های اندروید برای ۱-۲-۴-۴
۱۳۳ پنهان‌نگاری در اندروید ۳-۴-۴
۱۳۳ API های اندروید برای پنهان‌نگاری ۱-۳-۴-۴
۱۳۸ برنامه پیاده‌سازی شده به صورت تصویری ۴-۴-۴
۱۳۸ برنامه مشتری ۱-۴-۴-۴
۱۴۱ برنامه تاجر ۲-۴-۴-۴
۱۴۲ فصل ۵-۴ چکیده
۱۴۳ فصل ۵: نتیجه‌گیری و طرح پیشنهادها
۱۴۴ ۱-۵ نتیجه‌گیری
۱۴۶ ۲-۵ پیشنهادهایی برای کارهای آتی
۱۴۷ فهرست منابع و مأخذ
۱۵۳ Abstract

فهرست جدول‌ها

جدول ۱-۲: استانداردهای اصلی در تکنولوژی NFC.....	۲۱
جدول ۲-۲: تکنولوژی‌های کارت هوشمند مجاروتی غیر تماسی.....	۲۳
جدول ۳-۲: تعامل دو دستگاه NFC.....	۲۶
جدول ۴-۲: مقایسه انواع تگ در انجمن NFC [۵۹].....	۳۹
جدول ۵-۲: مقادیر رشته‌ی قالب نام نوع (TNF).....	۴۲
جدول ۶-۲: مثال‌های نوع رکوردی NDEF شناخته شده.....	۴۳
جدول ۷-۲: رمزنگاری بایت حالت.....	۴۵
جدول ۸-۲: ذخیره‌یک رکورد متنی.....	۴۵
جدول ۹-۲: معنی عبارات به کار گرفته شده [۴۲].....	۴۷
جدول ۱-۳: اجازه دسترسی در برنامه‌های اندروید.....	۹۶
جدول ۱-۴: پروتکل پرداخت برخط.....	۱۰۴
جدول ۲-۴: پروتکل پرداخت برخط.....	۱۰۷
جدول ۳-۴: کلاس‌های موجود در بسته android.nfc.....	۱۰۹
جدول ۴-۴: پشتیبانی TNF و نگاشت آن.....	۱۱۲
جدول ۵-۴: پشتیبانی RTD برای TNF_WELL_KNOWN و نگاشت آنها.....	۱۱۲
جدول ۱-۵: مقایسه روشهای امنیتی و راه‌حل‌های آنها.....	۱۴۵

فهرست شکل‌ها

- شکل ۱-۲: کارت هوشمند ملی ۱۰
- شکل ۲-۲: کارت هوشمند تماسی ۱۱
- شکل ۳-۲: کارت هوشمند غیرتماسی ۱۱
- شکل ۴-۲: طبقه‌بندی کارت‌های هوشمند ۱۲
- شکل ۵-۲: SDA ۱۴
- شکل ۶-۲: دیاگرام DDA ۱۵
- شکل ۷-۲: جریان تراکنش‌ها در EMV و ارتباط آن با مکانیسم‌های امنیتی ۱۸
- شکل ۸-۲: نگاهت استاندارد ISO/IEC ۱۴۴۴۳ و ISO/IEC ۷۸۱۶ و مدل سیستم‌های باز ارتباطی [۲۰] ۲۴
- شکل ۹-۲: تعامل دو شیء هوشمند NFC ۲۵
- شکل ۱۰-۲: حالت عملیاتی خواننده/نویسنده ۲۷
- شکل ۱۱-۲: مدل کلی استفاده در حالت عملیاتی خواننده/نویسنده ۲۹
- شکل ۱۲-۲: حالت عملیاتی نظیر به نظیر ۲۹
- شکل ۱۳-۲: مدل کلی استفاده در حالت عملیاتی نظیر به نظیر ۳۰
- شکل ۱۴-۲: حالت عملیاتی شبیه ساز کارت ۳۱
- شکل ۱۵-۲: مدل کلی استفاده در حالت عملیاتی شبیه ساز کارت ۳۱
- شکل ۱۶-۲: برنامه‌ی کاربردی حالت عملیاتی خواننده/نویسنده ۳۲
- شکل ۱۷-۲: برنامه‌ی کاربردی حالت عملیاتی نظیر به نظیر ۳۳
- شکل ۱۸-۲: کاربرد حالت عملیاتی شبیه ساز کارت ۳۵
- شکل ۱۹-۲: دستگاه تلفن همراه دارای قابلیت NFC [۵۹] ۳۶
- شکل ۲۰-۲: پیام NDEF ۴۰
- شکل ۲۱-۲: پرچم‌ها در پیام NDEF ۴۰
- شکل ۲۲-۲: رکورد در پیام NDEF [۵۹] ۴۱
- شکل ۲۳-۲: حالت نظیر به نظیر ۴۶
- شکل ۲۴-۲: فاز ثبت نام [۴۲] ۴۸
- شکل ۲۵-۲: فاز احراز هویت [۴۲] ۴۹
- شکل ۲۶-۲: گزینه‌های معماری امنیت NFC [۴۴] ۵۳

شکل ۲-۲۷: نمای توصیف شده از تلفن همراه NFC [۴۴]	۵۸
شکل ۲-۲۸: شنونده RF و ردیاب اسیلوسکوپ [۴۴]	۵۸
شکل ۲-۲۹: تنظیمات حمله فرد مداخله گر [۵۶]	۶۴
شکل ۲-۳۰: حمله به NFC اگر NFC بتواند با مرورگر ارتباط برقرار کند [۵۷]	۷۰
شکل ۲-۳۱: قرارداد کلید ویژه NFC [۵۶]	۷۳
شکل ۳-۱: دو زمینه اصلی در رمزنگاری [۶۰]	۸۰
شکل ۳-۲: چهار هدف رمزنگاری	۸۰
شکل ۳-۳: طبقه بندی الگوریتم‌های رمزنگاری	۸۱
شکل ۳-۴: الگوریتم AES	۸۳
شکل ۳-۵: شیفت کردن ردیف‌ها	۸۴
شکل ۳-۶: درهم کردن ستون‌ها	۸۴
شکل ۳-۷: اضافه کردن نوبت کلید	۸۵
شکل ۳-۸: رمزنگاری با کلید عمومی	۸۶
شکل ۳-۹: تصویر پوشاننده	۸۸
شکل ۳-۱۰: تصویر استگو	۸۹
شکل ۳-۱۱: انتقال یک تصویر محرمانه به وسیله نهمان نگاری	۸۹
شکل ۳-۱۲: مقایسه استفاده از تعداد بیت‌های گوناگون در پنهان نگاری به روش LSB	۹۱
شکل ۳-۱۳: لایه‌های اندروید	۹۲
شکل ۳-۱۴: فرآیند نصب برنامه اندروید	۹۳
شکل ۳-۱۵: برنامه اندروید	۹۴
شکل ۳-۱۶: اعلان دسترسی برنامه اندروید در فایل منیفست	۹۵
شکل ۳-۱۷: صفحه نمایش دسترسی برنامه	۹۶
شکل ۳-۱۸: معماری رمزنگاری سیستم	۹۷
شکل ۴-۱: وارد کردن بسته nfc به برنامه	۱۰۹
شکل ۴-۲: رسیدگی به نگ	۱۱۱
شکل ۴-۳: تعریف آدابتور برای برنامه	۱۱۷
شکل ۴-۴: آماده کردن داده NDEF	۱۱۸
شکل ۴-۵: دریافت پیام NDEF	۱۱۹
شکل ۴-۶: پردازش پیام NDEF	۱۲۰
شکل ۴-۷: بیم کردن دو دستگاه تلفن همراه	۱۲۳
شکل ۴-۸: ایجاد پیام NDEF	۱۲۴
شکل ۴-۹: جلوگیری از ارسال پیام‌های پیش فرض NDEF در فایل منیفست	۱۲۵
شکل ۴-۱۰: فراخوانی متد setNdefPushMessage() در متد onCreate()	۱۲۶

۱۲۶onNewIntent()	شکل ۴-۱۱ : متد
۱۲۶onResume()	شکل ۴-۱۲ : متد
۱۲۷processIntent()	شکل ۴-۱۳ : متد
۱۲۷getNdefMessages()	شکل ۴-۱۴ : متد
۱۲۸	شکل ۴-۱۵ : فایل منیفست(تعریف اینتننت فیلتر برای استفاده از NFC)
۱۳۰AES	شکل ۴-۱۶ : اضافه کردن بسته‌ها برای رمزنگاری AES
۱۳۱(getRawKey())	شکل ۴-۱۷ : کلاس EncodeDecodeAES(متد)
۱۳۱(رمزگذاری)	شکل ۴-۱۸ : کلاس EncodeDecodeAES(رمزگذاری)
۱۳۲(رمزگشایی)	شکل ۴-۱۹ : کلاس EncodeDecodeAES(رمزگشایی)
۱۳۲(EncodeDecodeAES())	شکل ۴-۲۰ : برنامه مشتری-AES (فراخوانی کلاس EncodeDecodeAES)
۱۳۴	شکل ۴-۲۱ : وارد کردن بسته‌ها برای پنهان‌نگاری
۱۳۵(LSB۲bit)	شکل ۴-۲۲ : برنامه مشتری-پنهان‌نگاری (فراخوانی متد encodeMessage داخل کلاس LSB۲bit)
۱۳۵(EncodeActivity)	شکل ۴-۲۳ : برنامه مشتری-پنهان‌نگاری (فراخوانی کلاس EncodeActivity)
۱۳۶(DecodeActivity)	شکل ۴-۲۴ : برنامه تاجر-پنهان‌نگاری (فراخوانی کلاس DecodeActivity)
۱۳۶(LSB۲bit)	شکل ۴-۲۵ : برنامه تاجر-پنهان‌نگاری (فراخوانی متد decodeMessage داخل کلاس LSB۲bit)
۱۳۷(EncodeDecodeAES)	شکل ۴-۲۶ : برنامه تاجر-AES (فراخوانی کلاس EncodeDecodeAES)
۱۳۷(EncodeDecodeAES())	شکل ۴-۲۷ : برنامه تاجر-AES (فراخوانی کلاس EncodeDecodeAES)
۱۳۸	شکل ۴-۲۸ : صفحه نمایش برنامه مشتری
۱۳۸	شکل ۴-۲۹ : صفحه نمایش برنامه مشتری(پر کردن ویرایش متن)
۱۳۹	شکل ۴-۳۰ : صفحه نمایش برنامه مشتری(برای استفاده از پنهان‌نگاری)
۱۳۹	شکل ۴-۳۱ : صفحه نمایش برنامه مشتری(برای استفاده از پنهان‌نگاری_انتخاب عکس از گالری)
۱۴۰	شکل ۴-۳۲ : صفحه نمایش برنامه مشتری(برای استفاده از پنهان‌نگاری)
۱۴۰	شکل ۴-۳۳ : بیم کردن دو دستگاه
۱۴۱	شکل ۴-۳۴ : صفحه نمایش برنامه تاجر
۱۴۱	شکل ۴-۳۵ : صفحه نمایش برنامه تاجر(در صورت استفاده از پنهان‌نگاری_انتخاب عکس رمز شده)
۱۴۲	شکل ۴-۳۶ : صفحه نمایش برنامه تاجر(استخراج پیام رمز شده از عکس)
۱۴۲	شکل ۴-۳۷ : صفحه نمایش برنامه تاجر(رمزگشایی)

فصل اول:

کلیات پژوهش

۱- کلیات پژوهش

۱-۱- مقدمه

فن‌آوری‌های اولیه تلفن همراه، از کاربردهای محدودی مانند ایجاد تماس و پیام تعریف شد و به سمت استفاده پیچیده‌تر رفت. رشد سریع دستگاه تلفن همراه، تحولی در ارتباطات بی‌سیم ایجاد کرد. کاربران به راحتی می‌توانند معاملات مختلف و انتقال اطلاعات از طریق دستگاه‌های تلفن همراه خود انجام دهند. تلفن‌های هوشمند، تلفن همراهی است که با قابلیت محاسبات پیچیده‌تر و یک سیستم عامل است. برای استفاده از ویژگی‌ها و امکانات تلفن‌های هوشمند، برنامه‌های کاربردی در محدوده سرگرمی (برنامه بازی) به تراکنش آنلاین (پرداخت غیرتماسی) طراحی شده است. تلفن‌های هوشمند را می‌توان برای انواع حالات تراکنش پرداخت، مانند هزینه پارکینگ، کرایه حمل‌ونقل استفاده کرد. مشتریان می‌توانند در طول راه، برای تسریع زمان خرید، از تلفن‌های هوشمند خود، به‌عنوان روش پرداخت به جای استفاده از روش سنتی (نقدی و سکه) استفاده کنند [۱]. یک فن‌آوری مهم برای پرداخت سیار ارتباط میدان نزدیک^۱ نامیده می‌شود [۲] و [۳].

ارتباط میدان نزدیک NFC ارتباطات برد کوتاه بین دستگاه‌ها و برچسب‌ها را قادر می‌سازد [۴] و [۵]. انتظار می‌رود که پرداخت از طریق NFC بازار انبوهی تا سال ۲۰۱۵ داشته باشد [۶]. این فن‌آوری، تا پایان سال ۲۰۱۶، حدود ۴۴۸ میلیون کاربر و ارزش کل تراکنش سالانه برای پرداخت‌های تلفن همراه به ۶۱۷ میلیارد دلار خواهد رسید. همچنین، در حال حاضر بسیاری از تولیدکنندگان بزرگ تلفن همراه، تراشه‌ی NFC را در گوشی‌ها جاسازی کردند.

^۱ Near Field Communication (NFC)

با این حال، آسیب‌پذیری در فن‌آوری‌های جدید در پرداخت و صنعت بانکداری هدفی برای هکرها و سازمان‌های جنایی خواهد بود. یک حمله موفق، ممکن است اعتبار ارائه‌دهنده پرداخت و یا بانک از دست برود و احتمال اعتماد به فن‌آوری جدید از بین برود. بنابراین ارائه‌دهنده پرداخت باید هدف از ساخت یک روش پرداخت NFC امن و مورد اعتماد دنبال کنند.

۱-۲ ضرورت پژوهش

آخرین تحقیقات نشان می‌دهد که در آینده نزدیک، حدود بیست کشور از تکنولوژی NFC، برای پرداخت استفاده خواهند کرد.

از آنجا که NFC برای کاربردهای حساس امنیتی مانند پرداخت و کنترل دسترسی استفاده می‌شود، امنیت NFC مسئله‌ی مهمی به شمار می‌رود. با این حال، پروتکل‌های در حال حاضر، به‌خودی‌خود حاوی چند اقدامات امنیتی است که این مسئولیت‌های امنیتی به توسعه‌دهنده‌ی برنامه‌ی NFC، به نرم‌افزار سیار اضافه می‌کنند. دانستن آسیب‌پذیری‌ها و حملات احتمالی از NFC در گوشی‌های هوشمند یک گام مهم در ایجاد برنامه‌های کاربردی امن‌تر است. هنوز در NFC آسیب‌پذیری وجود دارد [۷] و [۸]. تمرکز تحقیقات روی دستیابی به معاملات پرداخت امن و احراز هویت کاربر در محیط پرداخت‌های تجاری متداول است. راه‌حل‌های پیشنهادی فن‌آوری‌های مختلف موجود مانند نسل دوم تکنولوژی تلفن‌های بی‌سیم (G۲)، فن‌آوری تلفن‌های بی‌سیم نسل سوم (G۳) و کارت‌های هویت شهروندی و کلید عمومی زیرساخت (PKI) همراه با NFC برای تأمین امنیت قوی و سهولت استفاده است. این پایان‌نامه آسیب‌پذیری‌های NFC را بررسی کرده و سپس به ارائه راه‌کار عملی برای حفظ امنیت در پرداخت از طریق این تکنولوژی، می‌پردازد.

طبق انجمن رسمی NFC [۹]، این فن‌آوری جدید راه، به علت تعامل برد کوتاه تضمین نمود. حتی با وجود سطح امن، نمی‌توان استراق سمع را رد کرد، چراکه ارتباط از طریق فرکانس رادیویی است. روش‌های حمله به‌طور کلی برای نرم‌افزار منحصر به فردند، تکنیک‌های متداول صورت می‌گیرد. استراق سمع عمل مخفیانه گوش دادن به مکالمه خصوصی دیگران بدون رضایت آن‌ها است [۳].

۱-۳ اهداف و سؤالات پژوهش

هدف اصلی این پایان‌نامه، ارائه لایه امنیتی برای برنامه‌های NFC است. در راستای رسیدن به این هدف، اهداف فرعی زیر تعریف شده‌اند.

- شرح انواع پرداخت‌ها تماسی و غیر تماسی
- شرح مدل پیچیده NFC در ارتباط غیرتماسی از طریق تلفن همراه هوشمند.
- شرح آسیب‌پذیری‌های و تهدیدات NFC و راه‌های مقابله با آن
- شرح الگوریتم‌های مناسب برای NFC،
- ایجاد کانال امن از طریق الگوریتم‌های رمزنگاری متقارن و نامتقارن برای احراز هویت و پرداخت برخط و غیر برخط.
- شرح مختصر درباره سیستم عامل اندروید و بسته‌های مربوط به رمزنگاری
- پیاده‌سازی کانال امن از طریق رمزنگاری متقارن و پنهان‌نگاری.

اما سؤال‌هایی که این پایان‌نامه پاسخ می‌دهد:

- آیا می‌توان سیستم پرداخت از طریق NFC را در تلفن‌های همراه پیاده‌سازی کرد؟
- *بررسی حمله‌هایی که NFC را تهدید می‌کند؟
- *بهترین روش امنیتی برای مقابله با حملات پرداخت NFC کدام است؟
- *لایه امنیتی نرم‌افزاری مخصوص تلفن‌های همراه چگونه پیاده‌سازی می‌شود؟

۴-۱ جنبه جدید بودن و نوآوری پژوهش

بامطالعه منابع پژوهشی مشخص شد که تاکنون پژوهشی جامع در زمینه حملات و تهدیدات صورت گرفته در NFC انجام نشده و همچنین لایه‌های امنیتی فقط به صورت تئوری بیان شده و راهکار عملی روی تلفن هوشمند دارای قابلیت NFC، صورت نگرفته است. این پژوهش، دو روش جدید رمزنگاری، برای مصونیت پرداخت از حمله، برای استفاده از تلفن همراه در پرداخت را ارائه کرده است.

۴-۱-۱ روش پژوهش

دو سناریو در این پژوهش مطرح شده است:

- فروشگاه‌های زنجیره‌ای وجود دارد که فروشندگان آن‌ها دارای تلفن هوشمند با قابلیت پرداخت از طریق NFC، می‌باشند. مشتری برای خرید خود نیاز است که بلیتی خریداری کند تا بتواند از این فروشگاه خرید کند. فروشگاه برای او بلیتی صادر می‌کند که دارای شماره بلیت و رمز مشترک بین فروشگاه و مشتری است. وقتی مشتری خریدی را انجام می‌دهد وارد برنامه‌ی مربوط به خود شده و با زدن شماره بلیت و رمز آن دستگاه خود را به دستگاه فروشنده نزدیک می‌کند و پیامی بین آن دو ردوبدل می‌شود. برنامه فروشنده

باز شده و رمز را وارد می‌کند. در صورت صحت رمز، شماره بلیت در برنامه فروشنده ظاهر می‌شود که صحت هویت مشتری را بیان می‌کند. در برنامه مشتری ابتدا شماره بلیت با استفاده از الگوریتم رمزنگاری متقارن رمز شده و همچنین برای مخفی کردن پیام، از پنهان‌نگاری استفاده می‌کند. در برنامه فروشنده پیام رمزگشایی می‌شود. این سناریو را با استفاده از تلفن هوشمند Samsung galaxy s3 دارای تکنولوژی NFC پیاده‌سازی شد.

-پرداخت می‌تواند به صورت برخط و غیر برخط صورت گیرد. فروشنده و مشتری برای انجام عملیات پرداخت از طریق NFC، باید حسابی در بانک داشته باشد. بانک به او امضای دیجیتالی می‌دهد که در صورت انجام تراکنش، برای صحت احراز هویت خود برای طرف مقابل بفرستد.

برای خرید، ابتدا فروشنده پیامی که شامل مبلغ و امضای دیجیتالی صادر شده از بانک، را برای مشتری از طریق NFC، می‌فرستد.

در صورتی که پرداخت برخط باشد، مشتری چکی را برای بانک می‌فرستد تا در صورت داشتن مبلغ در حساب، بانک برای فروشنده پیام می‌دهد که این مبلغ به حساب او واریز شده است.

در صورتی که پرداخت غیر برخط باشد، مشتری در داخل برنامه خود این مبلغ را چک می‌کند که در صورت داشتن آن، چکی را برای فروشنده می‌فرستد تا بعد آن را به بانک بدهد و از او پول را واریز کند.

۱-۶ ساختار پژوهش

در این پژوهش به منظور ارائه روش‌های جدید در پرداخت امن، از طریق NFC، پنج فصل زیر تدوین شده است:

فصل اول، کلیات پژوهش: در این فصل به ضرورت و اهداف و سؤالات این پژوهش را معرفی می‌کند.

فصل دوم، مرور ادبیات پژوهش و کارهای مرتبط: ابتدا به انواع روش‌های پرداخت و سپس به پرداخت سیار و معرفی فن‌آوری NFC و کاربردهای آن و سپس آسیب‌پذیری‌های آن در پرداخت و در آخر به مروری از تحقیقات مربوط به حمله‌ها پرداخته خواهد شد.

فصل سوم، معرفی الگوریتم‌های استفاده شده در پژوهش: از جمله الگوریتم‌های رمزنگاری به کاررفته

در این، رمزنگاری متقارن AES و رمزنگاری با کلید عمومی و امضای دیجیتال است و سپس اشاره‌ای به پنهان‌نگاری خواهد پرداخت.

فصل چهارم، معرفی پروتکل‌های پیشنهادی و پیاده‌سازی یکی از آن‌ها با استفاده از زبان برنامه‌نویسی اندروید می‌پردازد.

فصل پنجم، نتیجه‌گیری و کارهای آتی: نتیجه‌ای از پژوهش و ارائه پیشنهادها برای کارهای آینده ارائه می‌دهد.

۱-۷ چکیده فصل

در این فصل به‌منظور معرفی پژوهش، کلیاتی از آن شامل: ضرورت انجام پژوهش، اهداف پژوهش، جنبه جدید بودن و روش پژوهش و ساختار آن بیان شد. در پایان فصل نیز ساختار کلی پایان‌نامه به‌طور مختصر توصیف شد.