مهندسی صنایع و مدیریت شریف، (تابستان ۱۳۹۳)
دوره‌ی ۱-۳۰، شماره‌ی ۱/۱، ص. ۲۵-۳۴

Original Article

بررسی راهکارهای مؤثر برای کاهش محدودیت‌های امنیتی و نقض حریم شخصی در استفاده از سیستم‌های RFID در ایران (موردکاوی: گذرنامه‌ی الکترونیکی)

نسیم نهاوندی * **(دانشیار)**
طیبه صباغی (کارشناس ارشد)
بخش مهندسی صنایع، دانشگاه تربیت مدرس

گذرنامه‌ی الکترونیکی یکی از کاربردهای تکنولوژی شناسایی از طریق امواج (RFID)[1]، به‌عنوان سند مهم شناسایی و احراز هویت است. با توجه به اهداف سازمان ایکائو مبنی بر مجهز شدن تمامی کشورها به گذرنامه‌ی الکترونیکی، افزایش امنیت و همچنین لزوم اجرای گذرنامه‌ی الکترونیکی در ایران، ضروری است تهدیدها و راهکارهای امنیتی گذرنامه‌ی الکترونیکی مورد تحقیق قرارگیرد. در این مقاله هدف بر آن است که برای اولین‌بار تهدیدهای امنیتی گذرنامه‌ی الکترونیکی بررسی و راهکارهای مربوطه پیشنهاد شوند. بدین‌منظور ابتدا تهدیدهای امنیتی و نقض حریم شخصی استخراج و سپس از طریق پرسش‌نامه راهکارهای مؤثر برای کاهش تهدیدها شناسایی می‌شوند. نتایج تحقیق نشان می‌دهد که مهم‌ترین مخاطرات تأثیرگذار بر گذرنامه‌ی الکترونیکی شنودگذاری، سرقت، جعل و افشای اطلاعات است؛ همچنین می‌توان راهکارهای تأیید اعتبار فعال، کنترل دسترسی مقدماتی و کنترل دسترسی پیشرفته را به‌عنوان گزینه‌های قابل استفاده و مؤثر در گذرنامه‌ی الکترونیکی به کار گرفت.

واژگان کلیدی: شناسایی از طریق امواج رادیویی، حریم شخصی، امنیت، گذرنامه‌ی الکترونیکی.

n_nahavandi@modares.ac.ir
sabbaghi_ty21@yahoo.com

۱. مقدمه

۱.۱. تکنولوژی RFID

با گسترش روزافزون تکنولوژی RFID، بسیاری از افراد تصور می‌کنند که با تکنولوژی جدیدی مواجه‌اند، در حالی که RFID از حدود سال ۱۹۷۰ مطرح بوده اما به‌دلیل قیمت بالای آن، تا سال‌های اخیر در مصارف تجاری کاربرد زیادی نداشته است. طبق بررسی‌های انجام شده، مفهوم RFID از جنگ جهانی دوم با کشف فنّاوری IFF [2] ــ که سازوکاری شبیه به RFID دارد ــ مطرح شده است. IFF روشی برای تشخیص هواپیماهای جنگی خودی یا بیگانه بود که توسط انگلیسی‌ها کشف و استفاده شد. فنّاوری RFID به‌شکل امروزیش، اولین‌بار توسط ماریو کاردلو[3] کشف شد، اگرچه تا سال ۱۹۷۰ به‌علت گرانی کاربرد تجاری نداشت.[۱و۲] تکنولوژی RFID، که غالباً با وال‌مارت[4] و سازمان دفاع آمریکا شناخته می‌شود، با توجه به بهبود سرعت، دقت، کارایی و امنیت انتقال داده‌ها نقش وسیعی در مدیریت زنجیره‌ی تأمین[5] پیدا کرده است.[۱و۳] از این فنّاوری می‌توان برای ردیابی کتاب‌های کتابخانه‌ها یا سایر مستندات، و نیز در پیگیری و شناخت داروها و مدیریت تجهیزات بیمارستانی و گذرنامه‌ی الکترونیکی بهره جست.[۴و۵]

در حقیقت سیستم RFID نوع ویژه‌یی از شبکه‌های سنسوری است که افراد یا اشیاء را از طریق فرکانس‌های رادیویی و به‌صورت بیسیم شناسایی می‌کند.[۳] این سیستم از دو بخش مهم «برچسب[6]» و «قرائت‌گر[7]» تشکیل شده است. برچسب متصل به شیئی است که قرار است ردیابی شود، و قرائت‌گر وسیله‌یی است که با تشخیص حضور برچسب‌های RFID در محیط، اطلاعات ذخیره شده در آنها را بازیابی می‌کند و در نهایت این اطلاعات را به یک سیستم رایانه‌یی گزارش می‌دهد. قرائت‌گرها با کمک برنامه‌های میان‌افزاری[8] با نرم‌افزارهای کاربردی ارتباط برقرار می‌کنند. در این میان آنتن‌هایی بین قرائت‌گر و برچسب وجود دارد که ارتباط بین این دو را تقویت می‌کند.[۲-۴،۶و۷] امروزه یکی از کاربردهای RFID تعبیه‌ی دائمی تراشه‌ی RFID در داخل وسایلی است که افراد آنها را با خود جابه‌جا می‌کنند، نظیر گذرنامه‌ی الکترونیکی، کارت‌های شناسایی و کارت‌های ATM. این کاربردهای جدید RFID از زمان تراکنش می‌کاهند، اگرچه برخلاف کاربردهای گذشته باعث ایجاد تهدیدهای جدید امنیتی و حریم شخصی برای افراد نیز می‌شوند.[۸] دلایل به وجود آمدن این ریسک‌ها عبارتند از:[۸]

۱. تراشه‌ها به‌صورت دائمی در اشیایی که معمولاً توسط افراد جابه‌جا می‌شوند تعبیه

* نویسنده مسئول
تاریخ: دریافت ۱۳۹۰/۹/۱۹، اصلاحیه ۱۳۹۱/۸/۲۰، پذیرش ۱۳۹۱/۹/۲۰.

می‌شوند و دسترسی به اطلاعات تراشه در هر لحظه ممکن است.

۲. اطلاعات ذخیره شده روی تراشه‌ها ثابت‌اند و می‌توان به‌آسانی آنها را به افراد لینک کرد.

۳. افراد ممکن است از وجود تراشه بی‌اطلاع باشند یا به‌علت عدم وضوح سیگنال مهاجم، مشخص نباشد که چه فردی در حال خواندن سیگنال است.

۴. از اشیایی که در آنها تراشه تعبیه شده ممکن است در مکان‌های عمومی استفاده شود. در این مکان‌ها امکان دسترسی افراد غیرمجاز بدون اطلاع فرد به اطلاعات تراشه وجود دارد.

۲. مخاطرات سیستم‌های RFID

در سیستم‌های RFID ــ همانند تمامی سیستم‌های اطلاعاتی ــ عمدتاً دو بحث امنیت سیستم‌ها و حریم خصوصی کاربران مورد حمله‌ی مهاجمین قرار می‌گیرد. در ادامه، تهدیدها و خطرات ویژه‌یی که سیستم‌های RFID با آن مواجه‌اند شرح می‌دهیم.[۹]

۱.۲. استراق سمع[۹]

در استراق سمع، هکرها مخفیانه اطلاعاتی را شنود می‌کنند که برچسب RFID از طریق کانال ارتباطی هوا به قرائت‌گر ارسال می‌کند. با توجه به غیرفعال بودن استراق سمع، مهاجم نمی‌تواند هیچ سیگنالی را به دست آورد و بنابراین تشخیص سیگنال بسیار دشوار است. اقدامات متقابل[۱۰] رایج غالباً عبارت است از رمزگذاری داده‌ها و استفاده از یک صفحه‌ی فلزی به‌منظور حفاظت از برچسب و قرائت‌گر در زمان تبادل اطلاعات. مثلاً در ایستگاه‌های کنترل مرزی، براثر انجام این اقدامات، هکرها نمی‌توانند از طریق استراق سمع سیگنالی را شنود کنند.

۲.۲. حملات تأخیری[۱۱]

در حمله‌ی تأخیری، مهاجم بین قرائت‌گر قانونی و برچسب قانونی سرقت‌شده ارتباطی ایجاد می‌کند. در سیستم RFID، اگر قرائت‌گر و برچسب به یکدیگر نزدیک باشند ارتباط بین آنها از طریق کانال ارتباطی که مهاجمین ایجاد کرده‌اند (معمولاً بی‌سیم) برقرار می‌شود. بدین طریق مهاجمین می‌توانند خودشان را در سیستم‌های کنترل دسترسی یا سیستم‌های پرداخت تأیید اعتبار کنند. تولیدکنندگان می‌توانند با استفاده از برچسب‌های بردکوتاه یا با حفاظت از آنها، مثلاً نگهداری درکیف‌های آلومینیومی، با این خطرات و تهدیدات مقابله کنند.

۳.۲. خوانش غیر مجاز برچسب[۱۲]

مهاجمین می‌توانند با استفاده از قرائت‌گر جعلی اطلاعات برچسب را بخوانند. آنها می‌توانند برد خوانش قرائت‌گر جعلی را نسبت به فاصله‌ی ارتباطی استاندارد چندین برابر گسترش دهند. افزون بر این، در این روش ساخت یک «قرائت‌گر با بردی وسیع» نسبتاً ارزان است. اقدام متقابل ویژه علیه خوانش غیرمجاز برچسب، استفاده از قرائت‌گر قانونی است. شروع انتقال پس از فعال‌شدن برچسب توسط کاربر روش دیگری است. همچنین توسعه‌دهندگان با انتقال اطلاعات حساس به یک پایگاه داده‌ی حفاظت شده در قسمت انتهایی سیستم، مانند سیستم اطلاعات دارویی Veri Med ریسک را کاهش می‌دهند. توسعه‌دهندگان در مواجهه با نگرانی‌های حاصل از خوانش‌های غیرقانونی، محتوای سبدهای خرید با برچسب RFID با استفاده از فرمان «kill» را به‌صورت دائمی غیرفعال می‌کنند. همچنین محققین طراحی برچسبی را پیشنهاد داده‌اند که به کاربر اجازه می‌دهد آن را به‌صورت فیزیکی تخریب کند.

۴.۲. جعل برچسب[۱۳]

در این روش مهاجمین یک برچسب RFID المثنی ــ کاملاً هم‌سایز یا مقداری بزرگ‌تر از اندازه‌ی اصلی، اما با همان عملکرد ــ می‌سازند. مهاجمین از تکثیر یافته‌ها برای دسترسی به نواحی محدود یا ممنوعه، نظیر تجاوز به اطلاعات خصوصی، استفاده می‌کنند. تأیید اعتبار برچسب[۱۴] از شبیه‌سازی جلوگیری می‌کند.

۵.۲. ردیابی افراد

در این روش مهاجمین با استفاده از تکنیک‌های مختلف، مانند نصب قرائت‌گرهای جعلی در درها یا به‌کارگیری وسایل استراق سمع در نزدیکی قرائت‌گرهای قانونی، جابه‌جایی برچسب را دنبال می‌کنند. در این مورد می‌توان با شیوه‌هایی چون استفاده از برچسب‌هایی با برد کوتاه[۱۵] یا پوشاندن برچسب‌ها، تأیید اعتبار قرائت‌گرها و غیر فعال کردن برچسب‌ها زمانی که قابل استفاده نیستند، با جابه‌جایی برچسب مقابله کرد.

همچنین تولیدکنندگان می‌توانند در مرحله‌ی طراحی برچسب نسبت به رمزگذاری یا تخمین فاصله‌ی بین برچسب و قرائت‌گر براساس نسبت سیگنال به نویز اقدام کنند.

۶.۲. تغییر محتویات برچسب[۱۶]

اگر برچسبی قابل نوشتن[۱۷] باشد، مهاجمین می‌توانند محتویات آن را تغییر دهند یا تخریب کنند، یا این که باعث شوند سیستم کنترل دسترسی اشتباهاً فرد مجاز را رد کند. توسعه‌دهندگان می‌توانند در برخی از برچسب‌های قابل نوشتن با از بین بردن دائمی یا موقت امکان نوشتن، از اطلاعات حافظه‌ی برچسب محافظت کنند یا از قرائت‌گرهایی استفاده کنند که از خوانش اطلاعات برچسب به‌عنوان یک دستور جلوگیری کنند.

۷.۲. تخریب فیزیکی برچسب[۱۸]

ساده‌ترین و ارزان‌ترین روش برای تخریب سیستم‌های RFID، انهدام فیزیکی برچسب‌هاست؛ مثلاً گرم کردن آنها داخل یک ماکروویو، ضربه‌زدن به آنها با یک برچسب و مانند آن. این رویکرد به‌ویژه هنگامی کاربرد دارد که از برچسب‌های RFID نه فقط به‌منظور اهداف شناسایی بلکه به‌منظور حفاظت از کالاها و اقلام در مقابل سرقت استفاده می‌کنند. همچنین مردمی که نگران حریم شخصی‌شان هستند ممکن است برچسب‌های RFID موجود در گذرنامه‌های الکترونیکی‌شان را ــ با این که علی‌رغم کارنکردن برچسب RFID هنوز معتبرند ــ تخریب کنند.

۸.۲. ارسال نویز و انسداد[۱۹]

مهاجم حمله‌ی انسداد را با استفاده از برچسب مسدودکننده[۲۰] انجام می‌دهد. این برچسب تعداد بی‌شماری برچسب را شبیه‌سازی می‌کند که باعث حمله‌ی سرویس امنیتی (DoS)[۲۱] می‌شود و درآن به‌صورت بی‌پایان، قرائت‌گر یک سری برچسب‌هایی را می‌خواند که حضور خارجی ندارند. از تکنیک انسداد می‌توان برای حفاظت حریم خصوصی مشتری بهره گرفت.

در ارسال نویز، مهاجمین ارتباطات سیستم RFID را با ایجاد یک نویز رادیویی ــ در همان فرکانس سیستم ــ فلج می‌کند. برچسب مسدودکننده و دستگاه‌های ارسال نویز به‌راحتی قابل اکتشاف و مکان‌یابی هستند و توسعه‌دهندگان می‌توانند اخطاردهنده‌های مناسبی روی سیستم نصب کنند.

۳. گذرنامه‌ی الکترونیکی

اقدامات اساسی ایالات متحده و سایر کشورها درخصوص دو تکنولوژی همزمان RFID و بیومتریک، باعث تولید نسل جدیدی از کارت‌های شناسایی هوشمند شده است. استفاده از این دو تکنولوژی در کاهش کلاهبرداری، تسهیل شناسایی افراد و ارتقاء امنیت مؤثر است، اگرچه مخاطرات جدیدی نیز با این تکنولوژی‌ها همراه است. به‌دلیل حساسیت بالای اطلاعات بیومتریک و فردی، افراد سودجو ممکن است انگیزه‌ی بالایی برای جعل گذرنامه یا سرقت اطلاعات[۲۲] آن داشته باشند که پیامدهای آن بسیار جدی است؛ مثلاً سرقت اطلاعات بیومتریک و فردی، ردیابی دارنده‌ی گذرنامه، عبور از مرز به‌صورت غیرقانونی.[۱۰و۱۱] در تراشه‌ی داخل گذرنامه همان اطلاعات گذرنامه‌ی سنتی ذخیره می‌شود و درنتیجه امنیت اسناد افزایش می‌یابد و شناسایی افراد مختلف برای مامورین مرزی آسانتر می‌شود.[۱۲]

۱.۳. تجهیزات فنی

گذرنامه‌ی الکترونیکی شامل یک صفحه کاغذ و یک تراشه‌ی RFID است. همانند کارت‌های هوشمند بدون تماس، در داخل جلد گذرنامه‌ی الکترونیکی یک تراشه‌ی RF تعبیه شده که اطلاعات مندرج روی صفحه‌ی اطلاعات گذرنامه (نام، تاریخ تولد، شماره گذرنامه و...)، عکس چهره (با فرمت jpg)، و داده‌هایی اختیاری مثل اثر انگشت و تصویر عنبیه را شامل می‌شود. این گذرنامه‌های الکترونیکی قابل خواندن توسط ماشین[۲۳] هستند و با اختصاص شناسه‌های بیومتریکی به آنها در تمام جهان قابل تفسیرند. تکنولوژی منتخب براساس استاندارد ایزو ۱۴۴۴۳، سری A,B، دارای تراشه‌ی RF با حافظه‌ی ۶۴KB است که با تراشه‌های غیرفعال مطابقت دارد و در فرکانس ۱۳٫۵۶MHz کار می‌کند و دارای هیچ منبع قدرتی نیست و توان مصرفی خود را از طریق سیگنال‌های تولیدشده به‌وسیله‌ی قرائت‌گر فراهم می‌کند. استاندارد واضحی برای دامنه‌ی خوانش تراشه وجود ندارد اما به‌طور معمول بیشترین دامنه‌ی خوانش اطلاعات از تراشه تا قرائت‌گر، ۴ اینچ (۱۰ cm) است. درگذرنامه‌های الکترونیکی برای جلوگیری از سرقت اطلاعات از یک پوشش فلزی به‌نام «قفس فارادی[۲۴]» استفاده شده است.[۸]

۲.۳. استانداردهای ایکائو

به‌دنبال حوادث ۱۱ سپتامبر ۲۰۰۱، کشورهای زیادی طرح‌های اتخاذ استاندارد جدید گذرنامه را که موجب افزایش امنیت اسناد مسافرتی است تسریع کردند. هدف این طرح‌ها اتخاذ تکنولوژی جدیدی است که متضمن جامعیت فرایند صدور گذرنامه باشد و توانایی مقامات مرزی را برای استقرار هویتِ دقیقِ دارندگان گذرنامه که به دنبال امتیاز ورود هستند، بهبود بخشد.

بنابراین سازمان ایکائو برای تشخیص هویت در سطح جهانی چهار ویژگی بیان کرده که پایه‌های اصلی گذرنامه‌ی الکترونیکی را تشکیل می‌دهند:[۱۳و۱۴]

ــ تشخیص هویت از طریق شناسه‌های بیومتریک: در این میان تشخیص و بازشناسی هویت از طریق چهره به‌عنوان شناسه‌ی بیومتریک اجباری و بهره‌گیری از اثر انگشت یا عنبیه به‌عنوان گزینه‌های اختیاری برای تشخیص هویت مسافران تعیین شد.

ــ انتخاب تراشه‌ی بدون تماس برای ذخیره‌ی اطلاعات: تراشه‌یی با حافظه‌ی بسیار بالا برای ذخیره‌سازی اطلاعات مربوط به دارنده‌ی گذرنامه و قابل خوانش توسط دستگاه‌های قرائت‌گر.

ــ ساختار منطقی داده‌ها[۲۵]: این ساختار در سراسر جهان برای حصول اطمینان از تفسیر و تعبیر یکسان از اطلاعات و داده‌های ذخیره شده درگذرنامه‌های قابل خوانش توسط دستگاه ابداع شده است.

ــ برای حفاظت از اطلاعات ذخیره‌شده در تراشه‌ی گذرنامه‌ی الکترونیکی، از تدابیر امنیتی زیرساخت کلید عمومی[۲۶] استفاده می‌شود. راهبری و مدیریت زیرساخت کلید عمومی در اختیار ایکائو خواهد بود.

خلاصه‌یی از استانداردهای امنیتی ایکائو در جدول ۱ ارائه شده است. عکس دیجیتالی از چهره، «مشخصه‌ی قابل تبادل جهانی[۲۷]» را مشخص می‌کند، بدین‌معنا که می‌توان از آن به‌عنوان استانداردی بین‌المللی برای سنجیدن بیومتریک بهره جست. در واقع، ایکائو این ویژگی را به‌عنوان حداقلی برای معرفی جهانی اجباری می‌داند. از اطلاعات عنبیه‌ی چشم و اثر انگشت ممکن است به‌صورت اختیاری در مراکز صلاحدید هر کشور استفاده شود.

جدول ۱. خلاصه‌یی از استانداردهای امنیتی ایکائو.[۱۰]

اهداف طرح امنیتی	نام طرح امنیتی	نوع داده
از تغییر اطلاعات تشخیص هویت دارنده‌ی گذرنامه جلوگیری می‌کند	تأیید اعتبار غیرفعال بیومتریک: عکس چهره	اجباری
از جعل اطلاعات محرمانه‌ی تشخیص هویت دارنده‌ی گذرنامه جلوگیری می‌کند	تأیید اعتبار فعال کنترل دسترسی مقدماتی بیومتریک: اثر انگشت	اختیاری

۳.۳. تهدیدهای امنیتی و حریم خصوصی درگذرنامه‌ی الکترونیکی

به دنبال استفاده‌ی روزافزون از تکنولوژی RFID در موارد مختلف نظیرگذرنامه‌ی الکترونیکی، که در آن تراشه تعبیه شده، نگرانی اذهان عمومی از ردیابی و افشاء مسائل خصوصی‌شان نیز افزایش یافته است.[۱۵]

در گذرنامه‌ی الکترونیکی تراشه‌هایی به‌صورت دائمی در وسایل افراد تعبیه می‌شود که نمی‌توان به‌آسانی آن را پاک یا غیرفعال کرد. درگذرنامه‌های الکترونیکی که اکثراً افراد جابه‌جا می‌کنند و در مکان‌های عمومی از آن بهره می‌برند، این موضوع فرصت‌های بیشتری برای سازمان‌ها و افراد سودجو در دسترسی به اطلاعات فراهم می‌آورد. این تراشه‌های دائمی اطلاعات ثابت، شامل شماره شناسایی تراشه یا اطلاعات شخصی که وابسته به فرد حامل شی است، را ذخیره می‌کنند. این اطلاعات عموماً در طول زندگی تغییر نمی‌کند و لذا فقط یکبار به افراد لینک می‌شوند و می‌توان مکرراً در شناسایی افراد از آنها استفاده کرد. بنابراین، چون از یک سو نمی‌توان حضور افراد را در مکان‌های عمومی محدود کرد، و از سوی دیگر تراشه‌ی RFID از راه دور قابل خوانش است و بدون حفاظت‌های امنیتی و بدون آگاهی افراد می‌توان به

جدول ۲. تهدیدهای مطرح در گذرنامه‌ی الکترونیکی.[۱۵]

موقعیت امنیتی	تهدیدها
دشواری در تشخیص عملکرد غیرفعال	استراق سمع
برد کوتاه اسکن افشای اطلاعات شخصی	اسکن مخفیانه
ردیابی غیر مجاز	ردیابی مخفیانه
امضای دیجیتالی نمی‌تواند با جعل گذرنامه مقابله کند	جعل و سرقت اطلاعات
سهل‌انگاری افراد	افشای اطلاعات بیومتریک

اطلاعات آنها دسترسی پیدا کرد، برای جلوگیری از نقض حریم خصوصی و افزایش امنیت باید راهکارهایی اندیشید. در جدول ۲ خطراتی که گذرنامه‌ی الکترونیکی با آنها مواجه است ذکر شده است.

سرقت اطلاعات و استراق سمع ممکن است در هر رده‌یی از کاربردهای RFID امکان‌پذیر باشد؛ این دو تهدید تعداد زیادی از تهدیدها را در کاربردهای جدید RFID ایجاد می‌کنند (کاربردهایی که در آنها اطلاعات شناسایی روی تراشه‌ی جاسازی شده در اشیا است). تراشه‌های RFID از فاصله‌ی دور قابل خوانش هستند و این ویژگی باعث بروز تهدیدهای امنیتی نظیر سرقت اطلاعات و استراق سمع توسط افراد سودجویی می‌شود که قرائت‌گر رادیویی دارند. سرقت اطلاعات زمانی رخ می‌دهد که اطلاعاتِ روی تراشه‌ی RF بدون اطلاع و رضایت شخص خوانده شود. با تقویت سامانه‌یی که به خواندن اطلاعات ذخیره شده در تراشه‌ی گذرنامه‌ی الکترونیکی از فاصله‌ی دور مبادرت می‌کند، می‌توان از فاصله‌ی ۳۰ متری به اطلاعات موجود در تراشه‌ی گذرنامه‌ی الکترونیکی دسترسی پیدا کرد. این کار را اصطلاحاً «استراق سمع» می‌نامند.

در بسیاری از کشورها سرقت یا استراق سمع نقض حریم خصوصی شهروندان تلقی می‌شود. قفس فارادی غالباً مقابله‌یی است در برابر اسکن مخفیانه‌ی RFID. در گذرنامه‌های الکترونیکی می‌توان با استفاده از قفس فارادی، با پوششی از مواد متالیک از نفوذ سیگنال‌های RFID جلوگیری کرد. موضوع گذرنامه‌های مجهز به قفس فارادی فقط توسط صاحب گذرنامه قابل اسکن است و بدین‌ترتیب حریم خصوصی‌شان در امان می‌ماند. این در حالی است که قفس فارادی از استراق سمع در ارتباط بین قرائت‌گر و گذرنامه‌ی الکترونیکی قانونی جلوگیری نمی‌کند.

برچسب‌های RFID به‌صورت مخفیانه قابل اسکن هستند که همان تهدید اسکن مخفیانه است. طبق دستورالعمل پایه‌یی ایکائو نیازی به ارتباطات رمزگذاری شده‌ی بین گذرنامه و قرائت‌گر نیست. بنابراین، در تراشه‌ی گذرنامه‌ی الکترونیکی حفاظت نشده، اسکن مخفیانه‌ی اطلاعات شخصی مانند شماره گذرنامه، تاریخ تولد و مکان تولد در یک دامنه‌ی کوتاه ممکن است.

ردیابی مخفیانه: در استاندارد ایزو ۱۴۴۴۳ برای تراشه‌ی RFID در گذرنامه‌های الکترونیکی، فهرستی از شماره‌های شناسایی تراشه[۲۸] روی پروتکل اولیه قید شده است. اگر این شماره شناسایی برای هر گذرنامه متفاوت باشد، آنگاه ردیابی حرکات دارنده‌ی گذرنامه به‌وسیله‌ی افراد غیرمجاز مقدور خواهد بود. ردیابی حتی بدون خواندن اطلاعات روی تراشه هم ممکن است. مشکل اصلی در گذرنامه‌های الکترونیکی، سرقت اطلاعات شخصی در تراشه‌ی گذرنامه (افشای اطلاعات بیومتریک) است. طبق استاندارد ایکائو تراشه‌ی RFID در گذرنامه‌ی الکترونیکی باید حاوی اطلاعاتی چون نام دارنده‌ی گذرنامه، تاریخ تولد و شماره‌ی گذرنامه و یک عکس دیجیتالی از شخص باشد. ایکائو همچنین بر اضافه کردن اطلاعات شناسایی بیشتر همچون اثرانگشت و تصویر عنبیه صحه گذاشته است.

۴.۳. راهکارهای امنیتی موجود برای تهدیدهای گذرنامه‌ی الکترونیکی

گذرنامه‌ی الکترونیکی یکی از بزرگ‌ترین و جالب‌ترین پروژه‌های جهانی در راستای استفاده از سیستم کارت هوشمند است. امنیت کارت‌های هوشمند با اجرای الگوریتم‌های رمزنگاری و رمزگذاری کلید عمومی، بیومتریک و استفاده از لایه‌ی محافظ یا همان پوشش فلزی فراهم می‌شود که تمامی موارد در گذرنامه‌ی الکترونیکی قابل استفاده است. ایکائو تکنیک‌های کنترلی و رمزگذاری زیر را برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی ذکر کرده است:[۱۰،۱۲،۱۵]

تأیید اعتبار غیرفعال. اطلاعات ذخیره‌شده در تراشه‌ی گذرنامه توسط کشور صادرکننده به‌صورت دیجیتالی امضا شده و باید قبل از استفاده از گذرنامه، امضای دیجیتالی آن چک شود. استفاده از این روش ثابت می‌کند که محتوای امنیتی سند و ساختارهای منطقی داده‌ها اصالت خود را حفظ کرده و دست‌کاری نشده‌اند.

معایب: با استفاده از این روش نمی‌توان از ایجاد نسخه‌ی مشابه و جایگزین ساختن تراشه‌ی اصلی با تراشه‌ی دیگر جلوگیری کرد. این روش مانع از دسترسی افراد غیرمجاز نمی‌شود و از به سرقت رفتن اطلاعات جلوگیری نمی‌کند.

تأیید اعتبار فعال: در استاندارد ایکائو استفاده از مشخصه‌ی امنیتی اختیاری تحت عنوان «تأیید اعتبار فعال» تعریف شده است. در حالی که کنترل دسترسی مقدماتی روش کاملاً محرمانه‌یی است، تأیید اعتبار فعال یک روش ضد جعل[۲۹] است یعنی از شبیه‌سازی تراشه جلوگیری می‌کند. تأیید اعتبار فعال از خوانش غیرمجاز اطلاعات داخل گذرنامه‌ی الکترونیکی جلوگیری نمی‌کند. تأیید اعتبار فعال بر رمزگذاری کلید عمومی[۳۰] تکیه دارد. تأیید اعتبار با داشتن کلید محرمانه‌ی گذرنامه‌ی الکترونیکی کار می‌کند. به‌طور مشابه کلید عمومی به‌عنوان بخشی از داده‌های امضا شده یا تأیید شده روی گذرنامه ذخیره می‌شود.

معایب: پیچیدگی‌هایی به همراه دارد. به تراشه‌های پردازشگر نیاز دارد.

کنترل دسترسی مقدماتی: کنترل دسترسی مقدماتی کم‌ترین تدبیر امنیتی لازمی است که دولت‌ها در صدور گذرنامه‌های الکترونیکی باید رعایت کنند. برای اطمینان از این که داده‌های برچسب فقط توسط قرائت‌گرهای معتبر قابل خوانش باشد، کنترل دسترسی مقدماتی یک جفت کلید رمزگذاری محرمانه را در تراشه‌ی گذرنامه ذخیره می‌کند (KENC, KMAC). زمانی که قرائت‌گر تلاش می‌کند گذرنامه را اسکن کند، کنترل دسترسی مقدماتی شناسایی جفت کلیدها و کلید session را اثبات می‌کند. اگر تأیید اعتبار شد، گذرنامه اطلاعاتش را نشان می‌دهد، در غیر این‌صورت قرائت‌گر اطلاعات را نامعتبر فرض می‌کند، و دست‌یابی به خوانش گذرنامه رد می‌شود. کلیدهای محرمانه ناشی از اطلاعات محدوده‌ی قابل خوانش گذرنامه ــ نظیر شماره‌ی گذرنامه که معمولاً ۹ کاراکتری است، تاریخ تولد و تاریخ انقضای گذرنامه ــ است.

کنترل دسترسی مقدماتی از سرقت اطلاعات و سوء استفاده از گذرنامه جلوگیری می‌کند و از استراق سمع با بهره‌گیری از دستگاه قرائت‌گر ممانعت می‌کند؛ یعنی هنگام

مبادله‌ی اطلاعات بین تراشه و سامانه‌ی مجاز، قرائت‌گر به‌صورت مخفی اطلاعات را رهگیری می‌کند.

معایب: از ایجاد نسخه‌یی مشابه یا جایگزین‌ساختن تراشه جلوگیری نمی‌کند. این نکته ایجاب می‌کند که ازگذرنامه‌ی متعارف نیز کپی گرفته شود و این باعث پیچیده‌تر شدن روند کار می‌شود. کنترل دسترسی مقدماتی نیازمند تراشه‌ی پردازش‌گر است.

کنترل دسترسی پیشرفته: ایکائو پیشنهاد می‌کند که دسترسی به داده‌های بیومتریک حساس، محدودتر شود. این امر از طریق رمزگذاری یا استفاده از کنترل دسترسی پیشرفته انجام‌پذیر است. اگرچه این مورد توسط ایکائو توصیه شده ولی ایکائو هیچ استانداردی در این مورد معرفی نکرده، و فقط بیان می‌دارد که این سازوکار مشابه کنترل دسترسی مقدماتی است با این تفاوت که در این سازوکار یک کلید دسترسی پیشرفته مورد استفاده قرار می‌گیرد. تعریف این کلید در اختیار کشور مربوطه است. از این سازوکار در محافظت از اطلاعات بیومتریک مثل اثر انگشت و اطلاعات عنبیه که درگذرنامه ذخیره شده، استفاده می‌شود. با استفاده از این سازوکار تضمین می‌شود که سیستم بازرسی فقط با اجازه‌ی محل صدور گذرنامه می‌تواند اطلاعات بیومتریک مثل اثر انگشت و اطلاعات عنبیه را بخواند. کنترل دسترسی پیشرفته اعتبار تراشه و قرائت‌گر، هر دو، را تأیید می‌کند.

سیستم بازرسی کشور «الف» یک گذرنامه‌ی الکترونیکی صادر شده از کشور «ب» را می‌بیند و می‌خواهد به اثر انگشت دسترسی داشته باشد. از کشور «ب» در مورد اجازه برای این دسترسی سؤال می‌شود.

سیستم بازرسی ابتدا اعتبار تراشه را تأیید می‌کند. در اینجا محافظت از ارتباط غیرتماسی بین ماشین الکترونیکی و سیستم بازرسی بهتر از کنترل دسترسی مقدماتی با استفاده از کلیدهای متقارن قویتر انجام می‌شود. سازوکار تبادل کلید مبتنی بر رمزنگاری غیرمتقارن شامل زوج کلید عمومی ـ خصوصی برای ماشین و سیستم بازرسی است. تأیید اعتبار تراشه از کلید عمومی ماشین استفاده کرده و آن را در حافظه‌ی امن خود ذخیره می‌کند. این سازوکار را می‌توان جایگزین تأیید اعتبار فعال کرد.

در تأیید اعتبار قرائت‌گر تضمین می‌شود که تنها قرائت‌گرهای مجاز به داده‌های بیومتریک دسترسی دارند. در اینجا زیرساخت کلید عمومی برای تأیید قرائت‌گر مورد استفاده قرار می‌گیرد. تأیید اعتبار قرائت‌گر در دو مرحله انجام می‌شود: ۱. سیستم بازرسی زنجیره‌یی از گواهی‌های تأیید شده توسط تراشه را ارائه می‌دهد. این زنجیره شامل گواهی سیستم بازرسی که توسط تأییدکننده امضا شده، گواهی تأییدکننده که توسط مقام تأیید گواهی کشور صادرکننده امضا شده، و گواهی تأیید کشور صادرکننده است. ۲. برای تأیید اعتبار قرائت‌گر، سیستم بازرسی داده‌های شناخته شده را امضا می‌کند و آن را به ماشین می‌فرستد. برای شکل‌گیری این امضا سیستم بازرسی باید از کلید خصوصی استفاده کند. ماشین صحت امضا را با استفاده از کلید عمومی که در مرحله‌ی قبل دریافت کرده تأیید می‌کند. وقتی این دو مرحله انجام، و تأیید گرفته شد گذرنامه‌ی الکترونیکی می‌تواند اطلاعات را آزاد کند.

معایب: کنترل دسترسی پیشرفته به مدیریت کلید عمومی نیاز دارد، از تهیه‌ی نسخه‌ی مشابه و جایگزینی تراشه جلوگیری نمی‌کند، به تهیه‌ی کپی از گذرنامه‌ی متعارف نیاز دارد، پیچیدگی‌های بیشتری دارد و نیازمند تراشه‌ی پردازشگر است.

رمزگذاری داده‌ها: این امر سبب افزایش ضریب امنیت شناسه‌های بیومتریک می‌شود و به تراشه‌ی پردازشگر نیاز ندارد.

معایب: به فرایند پیچیده‌ی خارج‌کردن کلید از حالت رمزی نیاز دارد و از تهیه‌ی نسخه‌ی مشابه یا جایگزین شدن تراشه جلوگیری نمی‌کند. به پیچیده‌ترشدن فرایند منتهی می‌شود.

استفاده از پوشش محافظ: یکی از ساده‌ترین اقدامات برای جلوگیری از خوانش غیر مجاز استفاده از قفس فارادی است. از مواد متالیک مانند آلومینیم که در مقابل امواج رادیویی کدر است می‌توان به‌عنوان قفس فارادی استفاده کرد؛ چرا که این مواد می‌توانند از خوانش اطلاعات تراشه جلوگیری کنند. پس می‌توان از لایه‌ی بسیار نازک فلزی مانند آلومینیم برای پوشش گذرنامه استفاده کرد. این لایه مانع از خوانش گذرنامه می‌شود. برای خوانش چنین گذرنامه‌یی حتماً باید گذرنامه به‌طور فیزیکی باز باشد. لذا این روش به غیر از موارد کنترلی، سطح ورود به حریم خصوصی را کاهش می‌دهد.

در این نوشتار تکنولوژی RFID و گذرنامه‌ی الکترونیکی به‌عنوان یکی از کاربردهای جدید آن معرفی می‌شود. سپس با توجه به این که در ایران هنوز گذرنامه‌ی الکترونیکی به‌طور فراگیر اجرا نشده و به بحث حریم خصوصی و موارد نقض آن پرداخته نشده، در این نوشتار برای اولین بار به بررسی مواردی پرداخته‌ایم که باعث نقض حریم خصوصی افراد درگذرنامه‌ی الکترونیکی می‌شوند. همچنین راهکارهای مقابله با این تهدیدها مورد بررسی قرار می‌گیرند.

۴. روش تحقیق

تحقیق حاضر یک تحقیق کاربردی، و طرح تحقیق از نوع پیمایشی است. برای تدوین مبانی نظری در این نوشتار، استفاده از مطالعات کتابخانه‌یی نظیر کتاب و مقاله‌های علمی و شبکه‌ی اینترنت اولویت داشته‌اند.

در مرحله‌ی نخست با مرور ادبیات موضوع عوامل مهم دخیل در نقض حریم خصوصی گذرنامه‌ی الکترونیکی استخراج، و راهکارهای مقابله با آن بررسی شد. برای سنجش راهکارهای به کارگرفته شده در این خصوص یک پرسش‌نامه طراحی، و با توزیع آن در سطح کارشناسان اطلاعات لازم جمع‌آوری شد. برای بررسی میدانی، پرسش‌نامه از طریق مصاحبه در اختیار ۳۵ خبره و کارشناس در زمینه‌ی RFID قرار گرفت. بعد زمانی تحقیق سال ۱۳۸۸ و بعد مکانی آن تعدادی از شرکت‌های فعال در زمینه‌ی RFID در شهر تهران است. در پایان این اطلاعات با روش‌های آماری استنباطی مورد تجزیه و تحلیل قرارگرفت و فرضیات در نظرگرفته شده برای هر یک از این عوامل آزموده شد. لازم به ذکر است:

- منابع جمع‌آوری داده قابل اعتماد بودند. این افراد کارشناسان صاحب‌نظر در زمینه‌ی RFID هستند.
- سؤالات تحقیق براساس تحقیقات پیشین مطرح شده است.
- پرسش‌نامه قبل از توزیع توسط افراد کارشناس تأیید شد.

سؤالات ۱ تا ۱۰ مربوط به یک سری سؤالات عمومی و میزان آشنایی افراد با RFID و بیومتریک و گذرنامه‌ی الکترونیکی است. سؤالات ۱۱ تا ۲۱ برای تعیین عوامل نگران‌کننده‌ی افراد درمورد گذرنامه‌ی الکترونیکی و حساسیت افراد از نقض حریم خصوصی آنهاست. در سؤال ۲۳ تهدیدهای گذرنامه‌ی الکترونیکی و در سؤال ۲۴ راهکارهای امنیتی ارائه شده درگذرنامه‌ی الکترونیکی گنجانده شده است. برای سنجش از یک مقیاس ۵ نقطه‌یی طیف لیکرت ـ از خیلی کم ۱ تا خیلی زیاد ۵ ـ استفاده شده است. به‌منظور اندازه‌گیری قابلیت اعتماد از روش آلفای کرونباخ و نیز از نرم افزار SPSS۱۵ استفاده شده است. میزان آلفای کرانباخ حاصل برابر ۰/۷۵ است که چون از ۰/۷ بیشتر است پایایی پرسش‌نامه تهیه شده تأیید می‌شود.

۵. یافته‌های تحقیق

پرسش‌نامه‌ی تحقیق توسط ۳۵ کارشناس و فرد خبره پر شده است. طبق نتایج به دست آمده میزان تمایل افراد به استفاده از تکنولوژی‌های جدید ۹۴٫۴ درصد، میزان نگرانی آنها نسبت به نقض حریم خصوصی‌شان ۹۷٫۱ درصد، میزان آشنایی‌شان با تکنولوژی RFID ۱۰۰ درصد، و میزان آشنایی با گذرنامه‌ی الکترونیکی ۸۲٫۸ درصد بوده است.[۱۶]

۱.۵. تعیین نرمال بودن مؤلفه‌های گذرنامه‌ی الکترونیک

برای بررسی نرمال بودن مؤلفه‌های تحت بررسی از آزمون کولموگروف ـ اسمیرنوف استفاده شده است. نتایج حاصل از این آزمون در جداول ۳ و ۴ لحاظ شده است. در اینجا آزمون با فرض زیر مورد بررسی قرارگرفت:

H۰: توزیع داده‌های مورد بررسی دارای توزیع نرمال است.

H۱: توزیع داده‌های مورد بررسی فاقد توزیع نرمال است.

میزان سطح معناداری مؤلفه‌های نقض حریم خصوصی، تأثیر شناسه‌های بیومتریک در افزایش امنیت، و تأثیرگذاری تکنولوژی RFID در گذرنامه‌ی الکترونیکی از میزان خطای نوع اول در سطح ۰٫۰۵ بیشتر است لذا فرض نخست برای این مؤلفه‌ها رد شد. بنابراین می‌توان از آزمون‌های پارامتری برای این مؤلفه‌ها استفاده کرد. اما سطح معناداری بقیه‌ی مؤلفه‌ها که بیان‌گر راهکارهای امنیتی گذرنامه‌ی الکترونیکی هستند از میزان خطای نوع اول در سطح ۰٫۰۵ کم‌تر است؛ لذا فرض نخست که بیان می‌دارد توزیع داده‌های تحت بررسی فاقد توزیع نرمال است، با ۹۵٪ اطمینان پذیرفته می‌شود. حال با مشخص شدن توزیع داده‌ها به بررسی فرضیه خواهیم پرداخت.

۲.۵. مقایسه‌ی مؤلفه‌های گذرنامه‌ی الکترونیکی

در این مرحله به مقایسه‌ی یک‌متغیره‌ی مؤلفه‌ها پرداخته‌ایم. هر سطر از جدول ۵ مربوط به یک مؤلفه است، و مقدار انحراف معیار و میانگین هر مؤلفه‌ی گذرنامه نیز

جدول ۳. نتایج نرمال بودن مؤلفه‌های گذرنامه‌ی الکترونیکی.

	عوامل مؤثر در نقض حریم خصوصی	تأثیر شناسه‌های بیومتریک در افزایش امنیت	تأثیرگذاری تکنولوژی RFID در گذرنامه
آماره‌ی کولموگروف ـ اسمیرنوف	٫۷۹۹	٫۶۰۴	٫۸۵۵
سطح معناداری	٫۵۴۶	٫۸۵۸	٫۴۵۷

جدول ۵. مقایسه‌ی مؤلفه‌های گذرنامه‌ی الکترونیکی.

فرضیات	تعداد مشاهدات	میانگین	انحراف معیار
میزان حساسیت افراد نسبت به نقض حریم خصوصی	۳۵	۳٫۴۷۳۵	۰٫۵۱۱۳۰
میزان تأثیر تکنولوژی RFID در گذرنامه‌ی الکترونیکی	۳۵	۳٫۴۲۷۱	۰٫۷۵۵۴۵

محاسبه شده است. انحراف معیار برای تعیین میزان پراکندگی جواب‌هاست و نشان می‌دهد که افراد در جواب‌دادن به سؤال‌ها هم‌سلیقه‌تر بوده‌اند.

برای بررسی میزان تأثیر تکنولوژی با توجه به جدول ۵، متوسط پاسخ‌های ارائه شده از طرف پاسخ‌دهندگان برای میزان حساسیت برابر ۳٫۴۷ با انحراف معیار ۰٫۵۱ است. این مقدار میانگین بیان‌کننده این نکته است که پاسخ‌گویان نسبت به نقض حریم خصوصی خود تا حد نسبتاً زیادی حساس‌اند. همچنین متوسط پاسخ‌های ارائه شده از طرف پاسخ‌دهندگان برای بررسی میزان تأثیر تکنولوژی RFID برابر ۳٫۴۲ با انحراف معیار ۰٫۷۵ است. این مقدار میانگین نیز بیان می‌دارد که پاسخ‌گویان تکنولوژی RFID را تا حد نسبتاً زیادی در گذرنامه تأثیرگذار می‌دانند.

۳.۵. تحلیل مؤلفه‌های گذرنامه‌ی الکترونیکی

برای تحلیل مؤلفه‌های گذرنامه‌ی الکترونیکی از آزمون t تک‌نمونه‌یی استفاده شده است. در آزمون t تک‌نمونه‌یی مقدار آزمون برابر ۳ (سطح پاسخ متوسط) در نظر گرفته شده است. به‌عبارت دیگر اگر متوسط پاسخ‌های ارائه شده از طرف پاسخ‌گویان به مؤلفه‌ی مربوطه از حد تعریف شده (یعنی ۳) بیشتر باشد بیان‌گر این نکته است که به‌طورکلی پاسخ‌گویان افراد را به این مؤلفه حساس می‌دانند. اما برای اثبات معناداری آزمون، نتایج آزمون t در جدول ۵ اعلام و تفسیر شده است. در حقیقت با انجام آزمون t اثبات یکی از فرضیات H۰ و H۱ بررسی می‌شود.

۱. افراد نسبت به نقض حریم خصوصی‌شان نگران‌اند.

H۰: افراد نسبت به نقض حریم خصوصی خود حساس نیستند. $(\overline{X} \leq ۳)$

H۱: افراد نسبت به نقض حریم خصوصی خود حساس‌اند. $(\overline{X} > ۳)$

چنان که در جدول ۶ مشاهده می‌شود میزان آماره‌ی t برابر ۵٫۴۷۸ با درجه آزادی ۳۴ و سطح معناداری صفر است. لذا فرض ۱ مبتنی بر این که افراد نسبت به نقض حریم خصوصی خود نگران‌اند با ۹۵٪ اطمینان اثبات می‌شود. چنان که ذکر شد برمبنای میانگین مشاهده شده میزان این تأثیرگذاری نسبتاً زیاد است.

۲. تکنولوژی RFID در گذرنامه تأثیرگذار است.

جدول ۴. نتایج نرمال بودن راهکارهای امنیتی در گذرنامه‌ی الکترونیکی.

	تأیید اعتبار غیرفعال	تأیید اعتبار فعال	کنترل دسترسی مقدماتی	کنترل دسترسی پیشرفته	رمزگذاری تصاویر بیومتریک	استفاده از راهنمای کلید عمومی
آماره‌ی کولموگروف ـ اسمیرنوف	۱٫۴۶۵	۱٫۶۹۶	۱٫۴۲۰	۱٫۵۱۰	۱٫۳۶۶	۱٫۳۶۹
سطح معناداری	٫۰۲۷	٫۰۰۶	٫۰۳۵	٫۰۲۱	٫۰۴۸	٫۰۴۷

جدول ۶. نتایج آزمون t تک‌نمونه‌یی.

مؤلفه‌های گذرنامه‌ی الکترونیکی	مقدار آزمون > ۳			
	T	درجه آزادی	سطح معناداری	تفاضل میانگین
میزان حساسیت افراد نسبت به نقض حریم خصوصی	۵٫۴۷۸	۳۴	٫۰۰۰	٫۴۷۳۴۷
میزان تأثیرگذاری تکنولوژی RFID در گذرنامه‌ی الکترونیکی	۳٫۳۴۵	۳۴	٫۰۰۲	٫۴۲۷۱۴

جدول ۷. نتایج رتبه‌بندی تهدیدهای گذرنامه‌ی الکترونیکی.

تهدیدهای گذرنامه‌ی الکترونیکی	متوسط رتبه
استراق سمع	۳٫۳۰
افشای اطلاعات بیومتریک	۳٫۰۶
سرقت و جعل اطلاعات	۲٫۹۳
اسکن مخفیانه	۲٫۸۹
ردیابی مخفیانه	۲٫۸۳

H۰: تکنولوژی RFID در گذرنامه تأثیرگذار نیست. ($\overline{X} \leq ۳$)

H۱: تکنولوژی RFID در گذرنامه تأثیرگذار است. ($\overline{X} > ۳$)

در این آزمون میزان آماره‌ی t برابر ۳٫۳۴۵ با درجه آزادی ۳۴ و سطح معناداری ۰٫۰۰۲ است. لذا فرض ۲ مبنی بر این که تکنولوژی RFID در گذرنامه تأثیرگذار است با ۹۵٪ اطمینان اثبات می‌شود.

۴.۵. رتبه‌بندی تهدیدهای گذرنامه‌ی الکترونیکی

برای بررسی میزان تأثیرگذاری و نحوه‌ی رتبه‌بندی عوامل مؤثر بر گذرنامه‌های الکترونیکی، بدان علت که پاسخ‌های ارائه شده براساس طیف لیکرت است، از آنالیز واریانس فریدمن استفاده می‌شود. در این تحلیل اثبات یکی از فرضیات زیر انجام می‌شود:

H۰: از نظر پاسخ‌دهندگان عوامل تأثیرگذار بر گذرنامه‌های الکترونیکی دارای اهمیت یکسان است.

H۱: از نظر پاسخ‌دهندگان عوامل تأثیرگذار بر گذرنامه‌های الکترونیکی دارای اهمیت یکسان نیست.

میزان آماره‌ی مجذورکا برای اثبات یکی از فرضیات فوق برابر ۵٫۰۱۸ با درجه آزادی ۴ و سطح معناداری ۰٫۲۸۵ است. چون سطح معناداری از میزان خطای نوع اول در سطح ۰٫۰۵ بیشتر است لذا فرض H۱ رد می‌شود و بنابراین عوامل اهمیت یکسان دارند. متوسط رتبه‌های به دست آمده برای متغیرها در جدول ۷ مشخص شده است.

چنان‌که مشاهده می‌شود ترتیب اولویت عوامل تأثیرگذار بر گذرنامه‌های الکترونیکی عبارت‌اند از: استراق سمع، افشای اطلاعات بیومتریک، سرقت و جعل اطلاعات، اسکن مخفیانه و ردیابی مخفیانه.

جدول ۸. مقایسه‌ی راهکارهای امنیتی.

راهکارهای امنیتی	تعداد مشاهدات	میانگین	انحراف معیار
تأیید اعتبار غیر فعال	۳۵	۴٫۱۱۴۳	٫۸۶۶۷۵
تأیید اعتبار فعال	۳۵	۴٫۲۵۷۱	٫۷۸۰۰۰
کنترل دسترسی مقدماتی	۳۵	۴٫۰۸۵۷	٫۹۱۹۴۴
کنترل دسترسی پیشرفته	۳۵	۴٫۱۴۲۹	٫۷۷۲۴۲
رمزگذاری تصاویر بیومتریک	۳۵	۴٫۰۲۸۶	٫۹۵۴۴۲
استفاده از راهنمای کلید عمومی	۳۵	۴٫۰۵۷۱	٫۸۷۲۵۵

۵.۵. تأثیرگذاری هر یک از راهکارهای ارائه شده در گذرنامه‌ی الکترونیکی

در جدول ۸ مقایسه‌ی راهکارهای امنیتی مشخص شده است. با توجه به جدول ۸ بیشترین میانگین پاسخ‌های ارائه شده به راهکار تأیید اعتبار فعال برابر ۴٫۲۵ با انحراف معیار ۰٫۷۸ است و کم‌ترین میانگین پاسخ‌های ارائه شده مربوط به راهکار رمزگذاری تصاویر بیومتریک و برابر ۴٫۰۲ با انحراف معیار ۰٫۹۵ است.

حال برای تعیین این که راهکارهای ارائه شده در گذرنامه‌ی الکترونیکی برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی مناسب است یا خیر، و به‌دلیل این که پاسخ‌های ارائه شده دارای توزیع نرمال نیستند، از آزمون ناپارامتری دوجمله‌یی استفاده می‌شود. در این آزمون تعداد پاسخ‌هایی که مقداری کم‌تر از ۳ (سطح متوسط) را ارائه کرده‌اند با تعداد پاسخ‌هایی که مقدار بیشتر از ۳ را ارائه کرده‌اند مقایسه می‌کنیم. به‌علاوه با مقایسه‌ی نسبت تعداد افراد با پاسخ کم‌تر از ۳ با مقدار ۰٫۶ (۶۰٪ افراد پاسخی کم‌تر از ۳ را ارائه کرده‌اند) فرض مورد نظر اثبات یا رد می‌گردد.

۱. تأیید اعتبار غیرفعال راهکاری مؤثر برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی است.

برای تحلیل، افراد به دو گروه تقسیم می‌شوند. گروه اول کسانی که جواب (فرقی ندارد، کم و خیلی کم) و گروه دوم کسانی هستند که جواب (زیاد و خیلی زیاد) داده‌اند. بنابراین موافقین نظر ما کسانی هستند که جواب (زیاد و خیلی زیاد) دادند، یعنی این تهدید تأثیر زیادی دارد. بقیه نظر مخالف دارند؛ یعنی تأثیر این تهدید کم است.

H۰: نسبت موافقین و مخالفین با تأثیرگذاری راهکار تأیید اعتبار غیرفعال برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی برابر است.

H۱: یکی از گروه‌ها (موافقین و مخالفین با تأثیرگذاری راهکار تأیید اعتبار غیرفعال برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی) بیشتر از ۶۰٪ از پاسخ‌ها را به خود اختصاص داده است.

با توجه به جدول ۹ چون میزان معناداری (صفر) از میزان خطای ۰٫۰۵ کم‌تر است لذا فرض نخست تأیید می‌شود. بنابراین بین نسبت موافقین و مخالفین با تأثیرگذاری راهکار تأیید اعتبار غیرفعال برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی اختلاف معناداری وجود دارد. چنان که مشخص است ۸۰٪ از پاسخ گویان بر این باورند که راهکار تأیید اعتبار غیرفعال به میزان زیادی برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی تأثیرگذار است.

جدول ۹. نتایج آزمون دوجمله‌یی بر راهکارهای امنیتی.

راهکارهای امنیتی	دسته	تعداد	نسبت مشاهده شده	نسبت آزمون	سطح معناداری
تأیید اعتبار غیرفعال	گروه ۱ <= ۳	۷	٫۲	٫۶	۰
	گروه ۲ > ۳	۲۸	٫۸		
تأیید اعتبار فعال	گروه ۱ <= ۳	۷	٫۲	٫۶	۰
	گروه ۲ > ۳	۲۸	٫۸		
کنترل دسترسی مقدماتی	گروه ۱ <= ۳	۶	٫۱۷	٫۶	۰
	گروه ۲ > ۳	۲۹	٫۸۳		
کنترل دسترسی پیشرفته	گروه ۱ <= ۳	۶	٫۱۷	٫۶	۰
	گروه ۲ > ۳	۲۹	٫۸۳		
رمزگذاری عکس دیجیتالی	گروه ۱ <= ۳	۹	٫۲۶	٫۶	۰
	گروه ۲ > ۳	۲۶	٫۷۴		
استفاده از راهنمای کلید عمومی	گروه ۱ <= ۳	۱۰	٫۲۸	٫۶	۰
	گروه ۲ > ۳	۲۵	٫۷۲		

۲. تأیید اعتبار فعال راهکاری مؤثر برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی است.

H۰: نسبت موافقین و مخالفین با تأثیرگذاری راهکار تأیید اعتبار فعال برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی برابر است.

H۱: یکی از گروه‌ها (موافقین و مخالفین با تأثیرگذاری راهکار تأیید اعتبار فعال برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی) بیشتر از ۶۰٪ از پاسخ‌ها را به خود اختصاص داده است.

با توجه به جدول ۹ چون میزان سطح معناداری (صفر) از میزان خطای ۰٫۰۵ کم‌تر است لذا فرض یک تأیید می‌شود. بنابراین بین نسبت موافقین و مخالفین با تأثیرگذاری راهکار تأیید اعتبار فعال برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی اختلاف معناداری وجود دارد. چنان که مشخص است ۸۰٪ از پاسخ گویان بر این باورند که راهکار تأیید اعتبار فعال به میزان زیادی برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی تأثیر دارد.

۳. کنترل دسترسی مقدماتی راهکاری مؤثر برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی است.

H۰: نسبت موافقین و مخالفین با تأثیرگذاری راهکار کنترل دسترسی مقدماتی برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی برابر است.

H۱: یکی از گروه‌ها (موافقین و مخالفین با تأثیرگذاری راهکار کنترل دسترسی مقدماتی برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی) بیشتر از ۶۰٪ از پاسخ‌ها را به خود اختصاص داده است.

با توجه به جدول ۹ چون میزان معناداری (صفر) از میزان خطای ۰٫۰۵ کم‌تر است لذا فرض نخست تأیید می‌شود. بنابراین بین نسبت موافقین و مخالفین با تأثیرگذاری راهکار کنترل دسترسی مقدماتی برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی اختلاف معناداری وجود دارد. چنان که مشخص است ۷۴٪ پاسخ‌گویان بر این باورند که راهکار کنترل دسترسی مقدماتی تا حد زیادی برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی تأثیرگذار است.

۴. کنترل دسترسی پیشرفته راهکاری مؤثر برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی است.

H۰: نسبت موافقین و مخالفین با تأثیرگذاری راهکار کنترل دسترسی پیشرفته برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی برابر است.

H۱: یکی از گروه‌ها (موافقین و مخالفین با تأثیرگذاری راهکار کنترل دسترسی پیشرفته برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی) بیشتر از ۶۰٪ از پاسخ‌ها را به خود اختصاص داده است.

با توجه به جدول ۹ چون میزان معناداری (صفر) از میزان خطای ۰٫۰۵ کم‌تر است لذا فرض نخست تأیید می‌شود. بنابراین بین نسبت موافقین و مخالفین با تأثیرگذاری راهکار کنترل دسترسی پیشرفته برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی اختلاف معناداری وجود دارد. چنان که مشخص است ۸۳٪ از پاسخ‌گویان بر این باورند که راهکار کنترل دسترسی پیشرفته به میزان زیادی برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی تأثیرگذار است.

۵. رمزگذاری تصاویر بیومتریک راهکاری مؤثر برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی است.

H۰: نسبت موافقین و مخالفین با تأثیرگذاری راهکار رمزگذاری عکس بیومتریک

دیجیتالی برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی برابر است.

H۱: یکی از گروه‌ها (موافقین و مخالفین با تأثیرگذاری راهکار رمزگذاری عکس بیومتریک دیجیتالی برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی) بیشتر از ۶۰٪ از پاسخ‌ها را به خود اختصاص داده است.

با توجه به جدول ۹ چون میزان سطح معناداری (صفر) از میزان خطای ۰٫۰۵ کم‌تر است لذا فرض نخست تأیید می‌شود. بنابراین بین نسبت موافقین و مخالفین با تأثیرگذاری رمزگذاری عکس بیومتریک دیجیتالی برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی اختلاف معناداری وجود دارد. چنان‌که مشخص است ۷۴٪ از پاسخ‌گویان بر این باورند که راهکار رمزگذاری عکس بیومتریک دیجیتالی به میزان زیادی برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی تأثیرگذار است.

۶. استفاده از راهنمای کلیدی عمومی راهکاری مؤثر برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی است.

H۰: نسبت موافقین و مخالفین با تأثیرگذاری راهکار استفاده از راهنمای کلیدی عمومی برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی برابر است.

H۱: یکی از گروه‌ها (موافقین و مخالفین با تأثیرگذاری راهکار استفاده از یک راهنمای کلیدی عمومی برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی) بیشتر از ۶۰٪ از پاسخ‌ها را به خود اختصاص داده است.

با توجه به جدول ۹ چون میزان سطح معناداری (صفر) از میزان خطای ۰٫۰۵ کم‌تر است لذا فرض نخست تأیید می‌شود. بنابراین بین نسبت موافقین و مخالفین با تأثیرگذاری راهکار استفاده از یک راهنمای کلیدی عمومی برای مقابله با تهدیدهای گذرنامه‌ی الکترونیکی اختلاف معناداری وجود دارد. چنان که مشخص است ۷۲٪ از پاسخ‌گویان بر این باورند که استفاده از یک راهنمای کلیدی عمومی تا حد زیادی بر مقابله با تهدیدهای گذرنامه‌ی الکترونیکی تأثیرگذار است.

۶.۵. رتبه‌بندی راهکارهای امنیتی در گذرنامه‌ی الکترونیکی

برای بررسی میزان اثرگذاری و نحوه‌ی رتبه‌بندی راهکارهای امنیتی گذرنامه‌های الکترونیکی، چون پاسخ‌های ارائه شده بر اساس طیف لیکرت است، از تحلیل واریانس فریدمن استفاده شده است. در این تحلیل یکی از فرضیات زیر اثبات می‌شود:

H۰: از نظر پاسخ‌دهندگان راهکارهای امنیتی گذرنامه‌های الکترونیکی دارای اهمیت یکسان است.

H۱: از نظر پاسخ‌دهندگان راهکارهای امنیتی گذرنامه‌های الکترونیکی دارای اهمیت یکسان نیست.

میزان آماره‌ی مجذورکا برای اثبات یکی از فرضیات فوق برابر ۴٫۸۶ با درجه آزادی ۵ و سطح معناداری ۰٫۴۳۳ است. چون میزان سطح معناداری از میزان خطای نوع اول در سطح ۰٫۰۵ بیشتر است لذا فرض H۱ رد می‌شود. بنابراین عوامل دارای اهمیت یکسان هستند. متوسط رتبه‌های به دست آمده برای متغیرها در جدول ۱۰ مشخص شده است.

جدول ۱۰. نتایج رتبه‌بندی راهکارهای امنیتی گذرنامه‌ی الکترونیکی.

راهکارهای امنیتی	متوسط رتبه
تأیید اعتبار فعال	۳٫۷۷
کنترل دسترسی مقدماتی	۳٫۵۴
کنترل دسترسی پیشرفته	۳٫۵۴
تأیید اعتبار غیرفعال	۳٫۵۰
رمزگذاری تصاویر بیومتریک	۳٫۴۴
استفاده از یک راهنمای کلید عمومی	۳٫۲۰

چنان که در جدول ۱۰ مشاهده می‌شود ترتیب اولویت راهکارهای امنیتی گذرنامه‌های الکترونیکی عبارت‌اند از: تأیید اعتبار فعال، کنترل دسترسی مقدماتی، کنترل دسترسی پیشرفته، تأیید اعتبار غیرفعال، رمزگذاری تصاویر بیومتریک و راهکار استفاده از یک راهنمای کلید عمومی. چنانچه مشاهده می‌شود متوسط رتبه راهکارها بسیار به هم نزدیک است که شاید ناشی از ضعف اطلاعات پاسخ‌دهندگان است. در صحبت با افراد خبره تأیید شد که تأیید اعتبار فعال، کنترل دسترسی مقدماتی و کنترل دسترسی پیشرفته و تأیید اعتبار غیرفعال راهکارهای امنیتی بسیار مهمی هستند و باید در گذرنامه‌های الکترونیکی از آنها بهره‌مند شد. بنابراین پیشنهاد می‌شود که به منظور جلوگیری از شبیه‌سازی تراشه و به‌عبارتی جعل آن از تأیید اعتبار فعال، به‌منظور پیشگیری از سرقت اطلاعات و استراق سمع از کنترل دسترسی مقدماتی، به‌منظور محدودیت دسترسی به داده‌های حساس بیومتریک از کنترل دسترسی پیشرفته و به‌منظور اثبات اعتبار داده‌ها از تأیید اعتبار غیرفعال استفاده شود.

۶. نتیجه‌گیری

با توجه به اهمیت و تأکید سازمان ایکائو مبنی بر بیومتریک کردن اسناد مسافرتی، اداره‌ی گذرنامه و روادید وزارت امور خارجه ایران به‌طور جدی مصمم به عملیاتی کردن گذرنامه‌های الکترونیکی کرده است. در داخل گذرنامه‌ی الکترونیکی تراشه‌یی تعبیه شده که اطلاعات شخصی و بیومتریک افراد در آن ذخیره می‌شود. به‌دلیل اهمیت و حساسیت بالای اطلاعات تراشه، امکان سوء استفاده از این اطلاعات محرمانه باعث نگرانی افراد از نقض حریم خصوصی آنها شده است. طبق نتایج تحقیق انجام شده، استفاده از تکنولوژی RFID و شناسه‌های بیومتریک در گذرنامه‌ی الکترونیکی در افزایش امنیت تأثیرگذارند. در این نوشتار برای اولین بار تهدیدهای امنیتی گذرنامه‌ی الکترونیکی بررسی و راهکارهای مربوطه پیشنهاد شدند.

طبق نتایج پرسش‌نامه، استراق سمع مهم‌ترین تهدید و بعد از آن افشای اطلاعات بیومتریک، سرقت و جعل اطلاعات، اسکن مخفیانه و ردیابی مخفیانه مهم‌ترین تهدیدهای گذرنامه‌ی الکترونیکی هستند. راهکارهای امنیتی متعددی در جهت حفظ حریم خصوصی و مقابله با تهدیدها در گذرنامه‌های الکترونیکی وجود دارد. با توجه به نتایج تحقیق انجام شده می‌توان از تأیید اعتبار فعال به‌عنوان گزینه اول، و سپس کنترل دسترسی مقدماتی و کنترل دسترسی پیشرفته به‌عنوان گزینه‌های مهم قابل استفاده و مؤثر در کاهش تهدیدهای گذرنامه‌ی الکترونیکی بهره گرفت.

ویژگی‌های الکترونیکی و بررسی تهدیدهای امنیتی و نقض حریم خصوصی و ارائه‌ی راهکارهای مقابله با تهدیدها در آنها از موضوعات تحقیقاتی پیشنهادی در آینده است.

پانوشت‌ها

1. Radio Frequency Identification
2. identification friend or foe (IFF)
3. Mario Cardullo
4. Wal-Mart
5. suplly chain managment
6. RFID tag
7. tag reader
8. middleware
9. eavesdropping
10. countermeasure
11. relay attacks
12. unauthorized tag reading
13. tag cloning
14. tag authentication
15. low-range
16. tag content changes
17. writeable
18. physical tag destruction
19. blocking and Jamming
20. blocker tag
21. denial of service
22. skimming
23. machine readable passport (MRP)
24. cage farady
25. logical data structure (LDS)
26. public key identification
27. global interchange feature
28. chip ID
29. anti-cloning
30. public-key

منابع (References)

1. Tajima, T. "Strategic value of RFID in supply chain management", *Sciencedirect*, **13**, pp. 261-273 (2007).
2. Roberts, C.M. "Radio frequency identification (RFID)", *Computers & Security*, **25**(1), pp. 18-26 (February 2006).
3. Xiao, Y., Yu, S. Ni., Janecek, Q. and Nordstad, C. "Radio frequency identification: Technologies, application, and research issues", *Wireless Communications and Mobile Computing*, **7**, pp. 457-472 (2006).
4. Garfinkel, S.L., Juels, A. and Pappu, R. "RFID privacy: An overview of problems and proposed solutions", *IEEE Security & Privacy*, **3**(3), pp. 34-43 (2005).
5. Juels, A. "RFID security and privacy: A research survey", *IEEE Journal on selected Areas in communications,* **24**(2), pp. 381-394 (2006).
6. Moghaddasi, S., *Principals of RFID and Its Applications*, First Edition, Shiraz, Rastar (2008).
7. Knospe, H. "RFID security", *Information Security Technical Report*, **9**, pp. 39-50 (2004).
8. Meingast, M. and King, D.K. "Embedded RFID and everyday things: A case study of the security and privacy risks of the U.S. e-passport", *IEEE International Conference on RFID*, pp. 7-14 (26-28 March 2007).
9. Rotter, P. "A framework for assessing RFID system security and privacy risks", *Pervasive Computing, IEEE,* **7**(2), pp. 70-77 (2008).
10. Juels, A., Molnar, D. and Wagner, D. "Security and privacy issues in e-Passports", *IEEE Transactions*, on Dependable and secure Computing, **4**(4), pp.74-88 (2005).
11. Schouten, B. and Jacobs, B. "Biometrics and their use in e-passports", *Image and Vision Computing,* **27**(3), pp. 305-312 (February 2009).
12. Kalman, G. and Noll, J. "On privacy protection in biometric passport", *IEEE Conference,* pp. 60-64 (2009).
13. ICAO, Document 9303, "Machine readble travel documents", (2004).
14. Liersch, I. "Electronic passports-from secure specifications to secure implementations", *Information Security Technical Report,* **14**(2), pp. 96-100 (2009).
15. Jeng, A.B. and Chen, L.Y. "How to enhance the security of e-passport", *proceedings of the English International Conference on Machine Learning and Cybernetics*, pp. 2922-2926 (2009).
16. Sabbaghi, T. "Solutions for reduction of security and privacy violation in RFID systems (Case Study: e-passport)", Master theses, Tarbiat Modares University (2010).