Passive Defence
Vol. 15, No. 3, Autumn 2024, Serial No. 59
ISSN: 2980-8030 , E-ISSN: 2008-6849

Providing a Framework of Solutions to Reduce the Vulnerability of Smart Cards

Amir Mohtarami* , Ali Jamshidi

*Assistant Professor, Department of Information Technology, Malek Ashtar University, Tehran, Iran

(Received: 20/01/2024, Revised: 28/04/2024, Accepted: 29/06/2024, Published: 26/10/2024)
DOR: 20.1001.1.20086849.1403.15.3.7.8

ABSTRACT

Nowadays, the provision of electronic services under the titles of business and electronic government has become very widespread and unavoidable. Smart cards are one of the most used tools in the process of providing electronic services. Regarding the expansion of the use of smart cards, the category of security and security vulnerability of this tool is equally important. In this research, our goal is to identify the most important vulnerabilities of this type of cards and extract solutions to reduce these vulnerabilities. For this purpose, while examining the types of smart card technologies, architecture, standards, as well as case studies in the field of threats and attacks applied to cards in the country and the world, a list of solutions to deal with these threats was extracted and then using the opinion of experts and implementation Friedman's test, solutions extracted, refined and in the form of four dimensions of software, hardware, operating system and standards, a framework for dealing with these vulnerabilities is presented, which can be considered as passive defense measures in this field. to be The results of this research have resulted in a set of 61 solutions in four areas of hardware, software, operating system and standards of smart cards, which can be noticed by developers and those in charge of smart cards at the national level.

Keywords: Smart Cards, Electronic Services, Vulnerability, Framework

This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

Publisher: Imam Hussein University © Authors

* Corresponding Author Email: mohtarami@mut.ac.ir

پدافند غیرعامل

سال پانزدهم، شماره ۳، پاییز ۱۴۰۳، (پیاپی ۵۹): صص ۹۵-۸۵

شاپای چاپی: ۶۹۴۹-۲۰۰۸ | **شاپای الکترونیکی:** ۸۰۳۰-۲۹۸۰

علمی – ترویجی

ارائه چارچوبی از راهکارهای کاهش آسیب پذیری کارت های هوشمند

امیر محترمی[1*]، علی جمشیدی دانا [2]

DOR: 20.1001.1.20086849.1403.15.3.7.8

تاریخ دریافت: ۱۴۰۲/۱۰/۳۰ تاریخ پذیرش: ۱۴۰۳/۰۴/۰۹

تاریخ بازنگری: ۱۴۰۳/۰۲/۰۹ تاریخ انتشار: ۱۴۰۳/۰۸/۰۵

چکیده

امروزه، ارائه خدمات الکترونیک با عناوین کسب‌وکار و دولت الکترونیک، بسیار فراگیر و گریزناپذیر شده است. کارت‌های هوشمند یکی از ابزارهای پر استفاده در فرایند ارائه خدمات الکترونیکی می باشند. نظر به گسترش استفاده ازکارت‌هایی هوشمند، به همان نسبت مقوله امنیت و آسیب پذیری امنیتی این ابزار از اهمیت برخوردار است. در این پژوهش، هدف ما شناسایی مهمترین آسیب پذیرهای این نوع از کارتها و استخراج راهکارهایی برای کاهش این آسیب پذیریها است. بدین منظور، ضمن بررسی انواع فناوریهای کارت هوشمند، معماری، استانداردها و همچنین مطالعات موردی در زمینه تهدید و حملات اعمال شده بر روی کارت‌ها در کشور و دنیا، فهرستی از راهکارهای مقابله با این تهدیدات استخراج شده و سپس با استفاده از نظر خبرگان و اجرای آزمون فریدمن، راهکارهای استخراج شده، پالایش و در قالب ابعاد چهارگانه تمهیدات نرم افزاری، سخت افزاری، سامانه عامل و استانداردها، چارچوبی از روشها و راهکارهای مقابله با این آسیب پذیری‌ها ارائه شده است که می تواند به عنوان اقدامات پدافند غیرعامل در این حوزه نیز در نظر گرفته شود. نتایج این پژوهش به مجموعه ای از ۶۱ راهکار در چهار حوزه سخت افزار، نرم افزار، سامانه عامل و استانداردهای کارت های هوشمند منتج شده است که بر اساس مطالعات موردی و همچنین استفاده از آزمون ناپارامتریک فریدمن اعتبارسنجی شده است. این چارچوب از راهکارها سامانه می‌تواند قابل توجه توسعه‌دهندگان و متولیان امر کارت هوشمند در کشور قرار بگیرد.

کلیدواژه‌ها: کارت‌های هوشمند، خدمات الکترونیک،آسیب‌پذیری، چارچوب

[1] استادیار، فناوری اطلاعات، دانشکده برق و کامپیوتر دانشگاه صنعتی مالک اشتر، تهران، ایران (mohtarami@mut.ac.ir)- نویسنده مسئول

[2] کارشناسی ارشد، مهندسی پدافند سایبری، دانشکده برق و کامپیوتر دانشگاه صنعتی مالک اشتر، تهران، ایران

* این مقاله یک مقاله با دسترسی آزاد است که تحت شرایط و ضوابط مجوز Creative Commons Attribution (CC BY) توزیع شده است.

© نویسندگان

ناشر: دانشگاه جامع امام حسین (ع)

۱- مقدمه

هنگامی که از اقتصاد اطلاعات و تحول دیجیتال در ارکان مختلف زندگی صحبت می شود، ارایه خدمات الکترونیک[1] پیش فرض و جزء محوری این تحولات در نظر گرفته می شود. این مساله در کشور ما که وجه غالب فعالیتها و خدمات، دولتی می باشد با مفهوم دولت الکترونیک بیشتر پیوند خورده است. دولت الکترونیک[2] به معنای ارایه خدمات سازمان های دولتی به شهروندان از طریق شبکه های رایانه ای (اینترنت) است[۱]. از مهمترین نتایج مورد انتظار از دولت الکترونیک افزایش رضایتمندی مردم از طریق افزایش سرعت، دقت و صرفه‌جویی در هزینه‌ها و ازجمله کاهش فساد اداری است[۲].

توسعه و گسترش کاربرد کارت‌های هوشمند[3] از جمله الزامات استقرار و تحقق برنامه های کاربردی دولت الکترونیک و بانکداری الکترونیک محسوب می شود. بنا براین، ممکن است هر فرد در دولت الکترونیک از چندین کارت از قبیل کارت‌های بانکی، کارت‌های پیش پرداختی مانند کارت مترو و اتوبوس، کارت ملی هوشمند، گواهینامه رانندگی، کارت سوخت، کارت ملی سلامت و ... استفاده نماید.

علاوه‌براین با توجه به ساختار کارت هوشمند و قابلیت ذخیره سازی اطلاعات، تبادل اطلاعات حساس مالی و یا شخصی، امنیت در حوزه کارتهای هوشمند به‌عنوان یکی از دغدغه‌های تولیدکنندگان و توسعه دهندگان کارت هوشمند می باشد. لذا با فراگیر شدن خدمات الکترونیک و همه گیر شدن استفاده از کارت‌های هوشمند، مقوله امنیت آن نیز به‌عنوان یک نیاز اساسی مطرح می‌شود.

از این رو شناسایی آسیب پذیری‌های این فناوری و تمهید راهکارهایی برای کاهش این آسیب ها گام مهمی برای گسترش امن این فناوری در خدمات الکترونیک روزمره است. بدیهی است در اجرای تمهیدات امنیتی باید مقوله هزینه/فایده را نیز در نظر گرفت.

در این مقاله، یافته های حاصل از پژوهشی ارائه می شود که هدف آن شناسایی راهکارهای کاهش آسیب پذیری کارتهای هوشمند و ارائه آن در قالب یک چارچوب مدون است. بنابراین، نخست پیشینه‌ای از فناوری کارت هوشمند و تهدیدات متناظر با آن ارائه می شود. سپس، روش تحقیق بکارگرفته شده بطور خلاصه تبیین می شود. به دنبال آن یافته های تحقیق در قالب چارچوبی مدون ارائه می شود و در نهایت یک نتیجه‌گیری و توصیه های سیاستی بیان می گردد.

۲- مفاهیم و پیشینه تحقیق

استفاده از کارتهای الکترونیکی را می توان از دهه ۵۰ میلادی ردگیری نمود. نخستین شکل آن، در قالب کارتهای پلاستیکی بود که به دلیل هزینه پایین این کارت‌ها که از جنس پلی وینیل کلراید[4] (پی-وی-سی) بودند، باعث شد تا به سرعت جایگزین کارت‌های کاغذی که تحمل تنش‌های فیزیکی و تغییرات آب و هوا را ندارند، شوند. اولین ارتقاء در این کارت‌ها با اضافه نمودن نوار مغناطیسی ذخیره داده به آنها که امکان ذخیره سازی اطلاعات را می‌داد پدید آمد. در سال ۱۹۷۰ و با پیشرفت چشمگیر در ریزپردازنده‌ها[5] و ترکیب آنها با حافظه‌های غیرفعال این امکان به وجود آمد تا از آنها در کارتهای هوشمند استفاده گردد. کارتهای هوشمند، امروزه در بسیاری از کاربردهایی که نیاز به نگهداری و انتقال امن اطلاعات داده‌ها، کنترل دسترسی به سامانه‌های رایانه‌ای و نیز کنترل دسترسی فیزیکی به محیط‌های خاص به‌عنوان کلید الکترونیکی وجود دارند، بکار می‌روند.

کارت هوشمند که با نامهای کارت چیپ‌دار یا کارتهای با مدار مجتمع هم شناخته می‌شوند کارتی است که بر روی آن مدار مجتمع نصب شده است. همچنین از این نوع کارت می‌توان به جای کارت اعتباری و کارت پول یا در سامانه‌های امنیتی رایانه‌ای، سامانه‌های تشخیص هویت و بسیاری موارد دیگر استفاده کرد. امروزه کاربردهای این فناوری در سطح دنیا در اکثر زمینه ها قابل مشاهده بوده و حتی این روند، رو به رشد است. بانکها، مراکز مخابراتی، سازمانهای دولتی، مراکز بهداشتی، مراکز ارایه خدمات، مراکز آموزشی، مراکز تفریحی و غیره از این دستاوردهای کاربردی این فناوری بهره می‌گیرند. با توجه به کاربردهایی که اشاره شده امنیت در کارتهای هوشمند اهمیت ویژه‌ای را ملزوم می‌کند. رمزنگاری در کارتهای هوشمند نیازی است که به هیچ وجه قابل انکار نیست.

کارتهای هوشمند شرایطی را برای دسترسی به اطلاعات خود اعمال میکنند تا از محتویات داده‌های موجود در فایل‌ها محافظت کنند. کاربران فقط در شرایطی میتوانند به نوشتن یا خواندن اطلاعات کارت اقدام کنند که شرایط دسترسی و مجوزهای لازم را داشته باشند [۳].

لزوما؛ کارت تراشه ریزپردازنده همان کارت هوشمند نیست. یک کارت ریزپردازنده متداول و غیراختصاصی می‌تواند امنیت منطقی را به همراه داشته باشد ولی این به تنهایی برای یک کارت هوشمند کافی نیست. مهاجمین می‌توانند با استفاده از تعدادی فنون/روش‌ها که تراشه را مستقیما مورد تهاجم قرار می‌دهد، و یا اطلاعات را از یک ابزار عملیاتی استخراج می‌کند، در

[1] Electronic Services
[2] e Government
[3] Smart Cards
[4] Polyvinyl chloride
[5] Microcontrollers

برابر امنیت منطقی کارت‌های تراشه ریزپردازنده مقاومت کنند. در حالی‌که ریزپردازنده‌ای که در کارت هوشمند استفاده می‌شود می‌بایست خیلی خاص طراحی شود، به‌گونه‌ای که در برابر دستکاری مقاوم باشد. بنابراین کارت هوشمند، کارتی است که تراشه ریزپردازنده‌ی آن در برابر دستکاری مقاوم بوده و در برابر حملات شناخته شده، اقدامات متقابل انجام می‌دهد، به همین دلیل کپی یا جعل آن سخت است. این کارت می‌تواند در انتقالات الکترونیکی خودکار وارد شده، داده‌ها را به صورت امن ذخیره نماید، و بعضی از پروتکل‌ها و الگوریتم‌های امن را اجرا نماید.

در این تحقیق منظور ما از کارت هوشمند، کارت تراشه ریزپردازنده‌ای است. اطلاعات مربوط به جزئیات امنیتی لحاظ شده در طراحی ریزتراشه نباید منتشر شده باشد. به گونه‌ای که با انجام اقدام متقابل در برابر حملات شناخته شده، در برابر دستکاری مقاومت می‌کند.

یک کارت، زمانی هوشمند نامیده می‌شود که بتواند در تراکنش‌های الکترونیکی به صورت خودکار(مکانیزه) وارد شده، اصولاً برای اضافه شدن امنیت استفاده می‌شود، به آسانی کپی یا جعل نمی‌شود، بتواند به صورت امن داده‌ها را نگهداری کند، و بتواند تعدادی الگوریتم‌ها و توابع امنیتی را اجرا کند [۴].

۲-۱- فناوری کارت‌های هوشمند

کارت هوشمند معمولا کارتی از جنس پی-وی-سی با ابعادی در حدود ۵/۵ در ۸/۵ سانتی‌متر است که بر روی آن یا در بین لایه‌های آن، تراشه‌های حافظه و ریزپردازنده برای ذخیره‌سازی داده‌ها و پردازش آنها قرارداده شده است. یک کارت هوشمند کامپیوتر کوچکی است که بر روی یک کارت پلاستیکی نصب شده است. قرار دادن یک تراشه در کارت به جای نوار مغناطیسی، آن را تبدیل به یک کارت هوشمند با کاربردهای گوناگون می‌نماید. این کارت‌ها به دلیل دارا بودن تراشه، قابلیت کنترل عملکرد را داشته و علاوه بر نگهداری اطلاعات شخصی و تجاری کاربر، امکان پردازش را نیز فراهم می‌نماید[۵].

اختراع کارت هوشمند را برای اولین بار فردی فرانسوی با نام رولاند مورنو در سال ۱۹۷۴ به ثبت رساند. از آن زمان به بعد، شرکت‌هایی نظیر بول[1]، هانیول[2]، موتورلا[3]، دراین زمینه به فعالیت پرداختند و در نتیجهٔ فعالیت‌های آنها، در سال ۱۹۷۹ اولین کارت هوشمند ریزپردازنده‌ای ساخته شد. اولین استاندارد برای کارت هوشمند در سال ۱۹۸۶ و با عنوان ISO ۱/۷۸۹۱۱۶ مطرح شد. استفاده از کارت هوشمند در سطح ملی برای نخستین بار در فرانسه در سال ۱۹۸۶ و برای کارت‌های اعتباری تلفن انجام گرفت. پس از آن، از اوایل دههٔ ۹۰ میلادی، استفاده از کارت‌های هوشمند درکشورهای مختلف رواج پیدا کرد و به تدریج کاربردهای جدیدی برای آن پیدا شد .

کارت‌هوشمند کارتی است که از یک ریزپردازنده و چیپ حافظه و یا فقط چیپ حافظه (بدون منطق برنامه‌پذیر) تشکیل شده است. کارت دارای ریزپردازنده می‌تواند اطلاعات روی کارت را اضافه، تغییر، حذف و مدیریت نماید، درحالیکه کارت فقط دارای حافظه (مانند کارت‌های اعتباری تلفن)، می‌تواند فقط یک عملیات از پیش تعریف شده را قبول کند .

کارت‌های هوشمند برخلاف کارت‌های نوار مغناطیسی، می‌توانند کلیه توابع عملیاتی و اطلاعات مربوطه را در خود داشته باشند، بنابراین در زمان انجام تراکنش نیاز به ارتباط با بانک اطلاعاتی نخواهد داشت. در حال حاضر سه گروه (بر اساس نوع تراشه بکار رفته در آن، حافظه و ریزپردازنده) از کارت‌های هوشمند در کاربردهای مختلف در دنیا و به صورت گسترده مورد استفاده قرار می‌گیرند:

۲-۱-۱-کارت‌های دارای ریزپردازنده مدار مجتمع

کارت‌های ریزپردازنده (همچنین عموما در صنعت بنام چیپ کارد[4] نامبرده می‌شود) حافظه ذخیره‌سازی و امنیت بیشتر ی را نسبت به کارت‌های نوار مغناطیسی فعلی ارائه می‌کند. این نوع کارت‌ها همچنین می‌توانند داده روی کارت را پردازش نمایند. نسل فعلی و تجاری این کارت‌ها دارای پردازنده ۸ بیتی، ۱۶ کیلوبایت حافظه فقط-خواندنی و ۵۱۲ بایت حافظه دسترسی تصادفی می‌باشند، که به آن‌ها قابلیت پردازشی معادل یک رایانه را می‌دهد .

این کارت‌ها برای کاربردهای بسیار گوناگونی استفاده می‌شوند، بخصوص کاربردهایی که در خود رمزنگاری داشته و نیاز به مدیریت و محاسبات روی اعداد بزرگ را دارند. بنابراین چیپ کارت‌ها زیرساخت کارت‌هایی که ابزار شناسایی دیجیتال و امن را در خود دارند، می‌باشند (شکل ۱). برخی از کاربردهای این نوع کارت‌ها عبارتند از :

- کارت‌های اعتباری و حاوی اطلاعات مالی
- کارت‌های امنیتی و دسترسی شبکه
- کارت‌های تلفن‌های سلولار (SIM Cards)

کارت‌های هوشمند همچنین بر اساس نحوه ارتباط با کارت‌خوان به صورت زیر دسته‌بندی شده است :

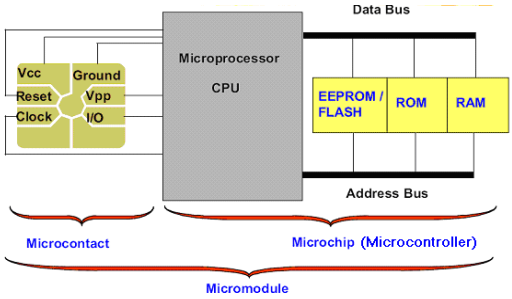
- کارت‌های هوشمند تماسی

برای استفاده از این قبیل کارت‌ها، باید اتصال فیزیکی بین کارت و دستگاه کارت‌خوان برقرار گردد. داده‌های موجود برروی کارت

[1] Bull
[2] Honeywell
[3] Motorola
[4] chip card

به صورت سریال به کارت‌خوان ارسال می‌شود و پس از پردازش، اطلاعات جدید از طریق همان پورت به روی کارت منتقل می‌شود. به عنوان نمونه، کارت‌های تلفن عمومی جزو این دسته محسوب می‌شوند. مشکل اصلی این قبیل کارت‌ها، خراب شدن کنتاکت‌های فلزی (محل‌های تماس) بر اثر عوامل خارجی نظیر ضربه و شرایط فیزیکی محیط است .

درشکل (۱) قسمت‌های موجود در نقاط تماس (کنتاکت‌ها) فلزی این نوع کارت نمایش داده شده است .



شکل (۱): ساختار میکرو ماژول کارت هوشمند و ارتباط آنها[۵]

• کارت‌های هوشمند غیرتماسی

در این نوع کارت هوشمند، ارتباط بین کارت و کارت‌خوان به‌صورت فیزیکی بر قرار نمی‌شود؛ بلکه از طریق میدان‌های الکترومغناطیسی و یا امواج RF صورت می‌گیرد. برای برقرای ارتباط، آنتن مخصوصی بین تراشه‌های کارت قرار داده شده است که در فاصله‌های کم، تا حدود ۵۰ سانتیمتر، می‌تواند ارتباط ایجاد کند. کاربرد اصلی این قبیل کارت‌ها در مواردی است که عملیات مورد نظر باید سریع انجام گیرد، به عنوان نمونه می‌توان به کارت‌های مترو اشاره کرد. مزیت اصلی این قبیل کارت‌ها علاوه بر سهولت استفاده، عمر طولانی‌تر و ضریب ایمنی بالاتر آن است؛ زیرا در این نوع کارت، تراشه به همراه آنتن در میان لایه‌های تشکیل‌دهندهٔ کارت قرار می‌گیرد .

• کارت‌های هوشمند ترکیبی

این نوع کارت ترکیبی از کارت‌های هوشمند تماسی و غیرتماسی است که با هر دو نوع دستگاه‌های کارت‌خوان سازگار است. از این نوع کارت‌ها برای ساخت کارت‌های چندمنظوره استفاده می شود.

۲-۱-۲- سامانه عامل

الگوها و برنامه‌ریزی‌های جدید در سامانه عامل کارت‌های هوشمند، سامانه عامل جاوا کارت[۱] است. این سامانه عامل توسط شرکت سان مایکروسامانه[۲] توسعه داده شده است و بعد از آن در انجمن جاواکارت گسترش یافته است. این سامانه عامل بسیار مورد توجه است زیرا در معماری برای طراحان و برنامه‌نویسان استقلال و آزادی عمل فراهم می‌آورد. همچنین برنامه‌های کاربردی مبتنی بر سامانه عامل جاوا می‌تواند برای هر کارت‌هوشمندی که سامانه عامل جاواکارت را پشتیبانی می‌کند استفاده گردد .

امروزه بیشتر کارت‌های هوشمند برای انجام ارتباط و عملیات برنامه‌ریزی شده ، سامانه عامل ویژه خود را استفاده می‌کنند. اما برای پشتیبانی واقعی از برنامه‌های کاربردی، سامانه‌های عامل کارت‌های هوشمند بر اساس عملیاتی که توسط استاندارد جهانی ISO-7816 فراهم گردیده، می‌باشند. با این حال برای انتقال برنامه‌ای که بر اساس تولیدات یک شرکت سازنده کارت فراهم شده، به سامانه تولیدکننده دیگر، کاری سخت و دشوار نیاز خواهد بود.

مزیت دیگر سامانه عامل جاواکارت این است که مفهوم انتشار سریع بارکنش برنامه کاربردی را پشتیبانی می‌کند. این قابلیت امکان بروزرسانی برنامه موجود در کارت بعد از توزیع کارت‌ها به کاربر را فراهم می‌نماید. نکته مهم این است که برای یک کاربرد خاص، فرد نیاز به کارت هوشمند دارد. اما نیازهای آتی وی، نیاز به تغییر برنامه‌های روی کارت را موجب خواهد شد که با این سامانه عامل ممکن خواهد بود .

سامانه عامل دیگری که برای کارت‌های هوشمند فراهم شده مالتوس[۳] یا سامانه عامل چند منظوره است. همچنان که از نام این سامانه برمی‌آید، این سامانه عامل قابلیت پشتیبانی چندین برنامه کاربردی را دارد. اما این سامانه عامل برای کاربردهایی با امنیت بالا طراحی شده است و موفق به کسب درجه عالی امنیت در استاندارد ITSec شده است. شرکت مایکروسافت نیز با توسعه سامانه کارت هوشمند ویندوزی[۴] در این مسیر قرار دارد .

۲-۲-پیشینه تحقیق

اولین کارتهای هوشمند طراحی شده از دو چیپ که یکی وظیفه پردازش و دیگری وظیفه ذخیره سازی را داشت طراحی و تولید شده بودند. این نوع ارتباط به سادگی به حمله کنندگان اجازه خرابکاری و به دست آوردن اطلاعات حساس روی کارت را می داد. بر همین اساس اولین حملات بر روی کارت‌های هوشمند در قبل از سال ۱۹۹۰ میلادی با لایه برداری و حل نمودن بسته بندی آن در اسید نیتریک بالای ۹۸ درصد و دسترسی فیزیکی به آدرسهای ارتباطی بین دو چیپ انجام شده است[۶].

دستکاری کردن ارتباط داده‌ها به وسیله جداسازی الکتریکی سطح ارتباط ماژول و سیم‌های ارتباط و سیم‌های مرتبط به ماژول، امکان دستکاری انتقال اطلاعات بین ترمینال و کارت را به طریق دلخواه برای مهاجم فراهم می‌نمود.

[1] JavaCard
[2] Sun Microsystem
[3] MULTOS(Multi-Application Operating System)
[4] Smart Card for Windows

پاک کردن حافظه خواندنی قابل پاک کردند با چراغ ماوراء بنفش، به وسیله تاباندن این نور به این نوع حافظه های امکان پاک کردن یا تغییر محتوای حافظه‌ها برای مهاجم فراهم می‌شد[۷].

برخی از مهاجمان به وسیله جایگزین نمودن مدارهای حافظه جهت رونوشت برداری و تقلید از کارکرد حافظه و ویژگی ایمنی شناسه رمزی به کار می‌بردند.

تحلیل کانال جانبی[1] یکی از مفید ترین روشهای رمز شکنی و به دست آوردن اطلاعات حساس از سامانههای الکترونیکی می باشد. به علت اینکه کارت‌های هوشمند در دسترس کاربر می باشد لذا مهاجم می تواند از هر نوع نشت فیزیکی چنین دستگاهی استفاده نموده و با تحلیل این نشت‌ها، کلید ذخیره شده در تراشه کارت را بیابد. اولین بار کوچر و همکاران در سال ۱۹۹۶ مفهوم تحلیل کانال جانبی را به کارت هوشمند تطبیق داد و بررسی های جامعی در این حوزه انجام داد[۹-۷].

یکی از حملاتی که مهاجمان بسیار از آن در جهت نفوذ در سامانههای رایانه ای استفاده می کنند، حملات تزریق خطا می‌باشد. در سال ۲۰۱۵ ریور و همکاران حمله تزریق خطا در کارت هوشمند را بررسی و به صورت نرم افزاری و سخت افزاری آن را شبیه سازی نموده است.در این حمله با ایجاد خطا در زمان پردازش کارت و تحلیل آن می توان کلید رمزنگاری را به دست آورد [۵,۸,۹,۱۶].

سامانه عامل کارتهای هوشمند نیز می تواند باعث ایجاد آسیب پذیری بر روی کارت هوشمند شوند، بهرنگ فولادی و همکاران در سال ۲۰۱۴ بر روی آسیب پذیری های کارتهای net. متمرکز شده و توانسته اند برخی از آسیب پذیری های موجود در این نوع کارتها را ارزیابی نموده و راهکارهایی نیز برای این رفع این آسیب پذیری‌ها ارایه نمایند[۱۰].

با توجه به ساختار پیاده سازی کارتهای هوشمند، در صورتی که پیاده سازی یک سامانه کارت هوشمند که مبتنی بر کارت، دستگاه خواننده کارت، ارتباطات و سرور می باشد به درستی پیکربندی نشده باشند می تواند باعث بروز آسیب پذیری های جدی در کارت هوشمند شده و امکان دستیابی مهاجمان به اطلاعات روی کارت هوشمند و یا اطلاعات تبادل شده بین سرور و کارت شوند. اشنیر و همکاران سابقه انواع حملات بر روی اجزای اصلی کارت هوشمند که متشکل از کارت، دستگاه خواننده کارت و ارتباط با سرور می باشد را بررسی نموده و راهکارهایی برای پیاده سازی کارت هوشمند با امنیت بیشتر ارایه نموده‌اند[۱۰].

یکی از متداول ترین روشهای ایجاد امنیت در کارت هوشمند، استفاده از شناسه شخصی به همراه کارت می باشد. امنیت در این حوزه مربوط به مخفی ماندن شناسه شخصی می‌باشد. در صورت به دست آمدن شناسه شخصی مهاجم می‌تواند کارت هوشمند سوء استفاده نماید. طی بررسی‌هایی که سینک و همکاران و همچنین ژانگ و همکاران انجام داده اند حملاتی را برای به دست آوردن شناسه شخصی را مانند حملات حدس زدن رمز عبور، حمله جعل سرور طراحی و پیاده سازی نموده‌اند. با مرور پژوهشهای مشابه در خصوص امن سازی و کاهش آسیب پذیری کارت‌های هوشمند، راه حل‌های متعددی اعم از استفاده از رمز عبور متغییر، استفاده از استگانوگرافی و ECC، رمزنگاری و احراز هویت بیومتریک و غیره را بررسی و ارایه نموده‌اند[۱۷-۱۳].

با این وجود، پرداختن به ابعاد مختلف آسیب پذیری و راهکارهای متناظر با این ابعاد مختلف که مجموعا بصورت یک چارچوب چند بعدی تنظیم می شود، امری است که نوآوری این پژوهش بوده و در پژوهشهای پیشین عمدتا بصورت تک متغیره یا تک بعدی مورد تحقیق قرار گرفته است.

۲-۲-۱- حملات متداول بر روی کارتهای هوشمند

در این بخش در ابتدا انواع حملات قابل اجرا بر روی کارت‌های هوشمند با استفاده از استانداردهای مختلف دسته‌بندی و توصیف شده است که در شکل (۲) تصویر درآمده است.

مراحل چرخه عمر یک کارت هوشمند را با در نظر گرفتن زمان‌بندی حمله‌های ممکن (طبق استاندارد ISO 10202-1) و طول عمر یک کارت هوشمند می‌توان در سه فاصله زمانی تقسیم‌بندی نمود.

- زمان طراحی و توسعه،
- زمان تولید،
- زمان استفاده از کارت.

از آنجایی که اکثر حملات شناخته شده در زمان استفاده از کارت انجام می‌شود، انواع این حملات مبتنی بر استاندارد ISO 13491-1 در سه دسته زیر قابل اجرا هستند.

- حمله در سطح اجتماع،
- حمله در سطح فیزیکی،
- حمله در سطح منطقی.

در عمل ممکن است انواع ترکیبی حمله‌ها نیز اتفاق بیافتد. به عنوان مثال یک حمله در سطح فیزیکی می‌تواند راهی برای اجرای حمله‌ای در سطح منطقی ایجاد نماید. مثال آن یک حمله از طریق تحلیل نقص تفاضلی است.

حمله‌های در سطح اجتماع حملاتی هستند که علیه افرادی که با کارت هوشمند کار می‌کنند هدایت می‌شود. این افراد طراحان تراشه که برای کارخانه‌های نیمه‌هادی کار می‌کنند یا طراحان نرم‌افزار و یا دارندگان کارت هستند. این حملات توسط روش‌های سازماندهی شده قابل پیشگیری هستند. به طور مثال قرار دادن صفحاتی برای جلوگیری از خوانده شدن عدد PIN در

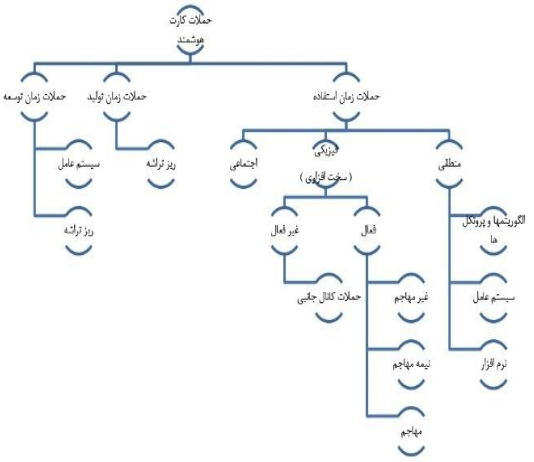
[1] Side Channel Analysis

طرفین صفحه کلید یک روش عمومی است.

از آنجایی که برای اجرای حملات روی کارت‌های هوشمند در سطح فیزیکی، لزوما نیاز به دسترسی فیزیکی به سخت‌افزار میکروکنترلر کارت هوشمند است، معمولاً نیاز به تجهیزات فنی خاص دارند. چنین حمله‌هایی می‌توانند ایستا و یا پویا باشند. ایستا به آن معنی است که هیچ توانی به میکروکنترلر اعمال نمی‌شود و پویا بر روی میکروکنترلرِ در حال عملکرد، اجرا می‌شود. در حمله‌های ایستای فیزیکی هیچگونه محدودیت زمانی به حمله کننده‌ای که عمل خود را در مکانش اجرا می‌کند، اعمال نمی‌شود؛ اما در حمله پویا تحلیل‌گر می‌بایست به تجهیزات موثر برای اکتساب و ارزیابی داده‌ها دسترسی داشته باشد.

تاکنون اکثر حمله‌های موفق شناخته شده روی کارت‌های هوشمند در سطح منطقی بوده‌اند. این حمله‌ها غالبا از ایده‌های ناب و خلاق یا محاسبات محض به‌دست می‌آیند. این دسته شامل تحلیل‌های کلاسیک می‌شوند؛ مانند حمله‌هایی که از نقص‌های شناخته شده‌ی سیستم‌عامل‌های کارت هوشمند بهره می‌گیرند و یا برنامه‌های اسب‌های تروا که در کدهای اجرایی برنامه‌های کاربردی کارت‌های هوشمند وجود دارند .

حمله‌های فیزیکی (سخت‌افزاری) که در انواع فعال و غیرفعال انجام می‌شوند، شامل انواع تحلیل‌های کانال جانبی[1]، روش‌های مهاجم۲ , روش‌های نیمه مهاجم[3]، و روش‌های غیرمهاجم[4] است که معمولاً بر روی سخت‌افزار کارت هوشمند اعمال می‌گردند و هر تکنیک آن در دو حالت ایستا و پویا قابل اجرا است. حمله‌های منطقی نیز معمولاً بر روی الگوریتم‌ها و پروتکل‌های بکار رفته اعمال شده و نرم‌افزار و سیستم‌عامل کارت را مورد تهدید قرار می‌دهند.

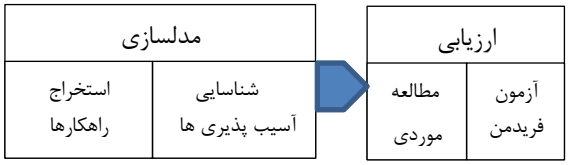


شکل (۲): طبقه‌بندی حملات قابل اجرا بر روی کارت‌های هوشمند

[1] Side Channel Attack
[2] Invasive Attack
[3] Semi Invasive Attack
[4] Non Invasive Attack

۳- روش تحقیق

در این پژوهش، دو مرحله اصلی دنبال شده است. (۱) مرحله مدلسازی که خود نیازمند نخست، شناسایی تهدیدات و آسیب پذیریهای متصور بر کارتهای هوشمند و دوم، استخراج راهکارهی مقابله با این آسیب پذیریها است (۲) مرحله ارزیابی که به دنبال اعتبارسنجی راهکارها و چارچوب به دست آمده است.



شکل (۳): مراحل و گامهای پژوهش

اطلاعات مورد نیاز در مرحله مدل‌سازی از مطالعات کتابخانه ای، از جمله کنفرانس ها و ژورنال های بین المللی، کتب مرجع و استانداردهای موجود در بازه زمانی ۱۹۹۸ الی ۲۰۲۲ استخراج گردید. همچنین، در مرحله ارزیابی راهکارها، با استفاده از شواهد موردی درخصوص اسیب پذیری ها و حملات کارتهای هوشمند و تطبیق موارد با راهکارهای ارائه شده، چارچوب ارایه شده، اعتبارسنجی گردید.

جدول (۱): مراحل تحقیق

فاز	فعالیت	روش
فاز مدل سازی	مطالعه و جمع آوری آسیب پذیری های شناخته شده	شناسایی و استخراج آسیب پذیریها از پژوهشهای پیشین و منابع علمی و تجربی
	بررسی و ارائه راهکارهای عملی برای رفع آسیب پذیری ها و یا کاهش آنها	تحلیل آسیب پذیری و استخراج راهکارها
فاز ارزیابی	ارزیابی نهایی	مطالعه موردی و تطبیق موارد با چارچوب ارائه شده آزمون فریدمن بر اساس نظر خبرگان

جامعه آماری تحقیق حاضر کلیه خبرگان حوزه کارتهای هوشمند است که به روش نمونه‌گیری غیر احتمالی گلوله برفی تعداد ۱۸ نفر مشخص و نظرخواهی لازم از طریق پرسشنامه صورت گرفت. توضیح بیشتر اینکه در این روش همه اعضا شانس انتخاب شدن یکسان ندارند و شانس هر عضو نیز مشخص نیست و به این صورت عمل می شود که فرد آینده نمونه از طریق راهنمایی افراد سابق نمونه انتخاب می‌شود و حجم نمونه مانند یک گلوله برفی کم کم بزرگ و بزرگ تر می شود و علت انتخاب این روش در نمونه گیری پژوهش حاضر آن بود که جامعه خبرگان حوزه کارتهای هوشمند یک جامعه پنهان بود.

روش گرد آوری اطلاعات- گردآوری اطلاعات در تحقیق حاضر شامل دو مرحله شد که به تناسب هر یک از مراحل از روش مخصوصی استفاده شد. مرحله اول جمع آوری اطلاعات و تئوری های مبانی نظری است که از روش کتابخانه ای استفاده شد و مرحله دوم جمع آوری داده های متناسب با متغیرهای مورد بررسی است که از روش دلفی استفاده شد.

ابزار گردآوری داده‌ها (اطلاعات)- از آنجا که گردآوری اطلاعات در پژوهش حاضر شامل دو مرحله شد، به تناسب هر یک از مراحل از ابزار مخصوصی نیز استفاده شده است. مرحله اول جمع آوری اطلاعات و تئوری های مبانی نظری است که از فیش و دفترچه یادداشت به عنوان ابزار استفاده شد و در بخش دوم که مربوط به جمع آوری نظرات جامعه خبرگان حوزه کارتهای هوشمند بود از پرسشنامه محقیق ساخته استفاده شد که در ادامه معرفی می‌شود:

پرسشنامه از ۶۶ سوال تشکیل شده، ۵ سوال عمومی در مورد دموگرافی پاسخ دهندگان و ۶۱ سوال در بررسی راهکارهای چهار حوزه سخت افزار، نرم افزار، سیستم عامل و استاندارد جهت کاهش آسیب پذیری کارتهای هوشمند. که در ادامه و در جدول (۲) خصوصیات دیگر پرسشنامه بیان شده است.

جدول (۲): توضیحات پرسشنامه بررسی راهکارهای کاهش آسیب پذیری کارتهای هوشمند

شرح		سوالات اختصاص داده شده	پایایی محاسبه شده با آلفای کرونباخ
ابعاد بررسی راهکار	سوالات عمومی	۵ سوال بدون شماره	۰۰۰۰
	حوزه سخت افزاری	۲۱ سوال از شماره ۱ تا ۲۱	۰/۸۴۲
	حوزه سیستم عامل	۱۵ سوال از شماره ۲۲ تا ۳۶	۰/۸۴۴
	حوزه نرم افزاری	۱۱ سوال از شماره ۳۷ تا ۴۷	۰/۸۱۸
	حوزه استاندارد	۱۴ سوال از شماره ۴۸ تا ۶۱	۰/۸۰۵
پایایی کلی پرسشنامه = ۰/۷۸۹			

در این پرسشنامه از روش روایی محتوا برای اطمینان از درستی ابزار اندازه گیری استفاده شده است به اینصورت که با استفاده از نظرات استاد راهنما، متخصصان و کارشناسان حوزه کارتهای هوشمند، مطالعه پرسشنامه های مشابه و همچنین توزیع ابتدایی پرسشنامه بین تعدادی از جامعه آماری و اعمال نظرات اصلاحی آنان و پس از رفع ابهام در سوالات، پرسشنامه نهایی طراحی، بومی سازی و تهیه گردید. همچنین به منظور سنجش پایایی از نرم‌افزار SPSS و شاخص ضریب آلفای کرونباخ استفاده شد که به دلیل بیشتر بودن ضریب آلفا از مقدار ۰/۷۰، تمامی مولفه های مورد مطالعه از اعتبار کافی برخوردار بودند. ضریب آلفا در مورد کل پرسشنامه نشان دهنده شانس و تصادف نبوده، بلکه به خاطر اثر متغیری می‌باشد که مورد آزمون قرار گرفته است. زیرا اولاً آنچه را که محقق در نظر داشته است دقیقاً سنجیده است و ثانیاً برداشت ذهنی تمام پاسخگویان از آن یکی بوده است.

روش تجزیه و تحلیل و اعتبارسنجی- تجزیه و تحلیل اطلاعات در تحقیق حاضر به دو روش توصیفی و استنباطی صورت گرفته است. در بخش توصیفی به ارائه دمگرافی خبرگان مورد بررسی پرداخته شده است و در بخش استنباطی به رتبه بندی راهکارهای کاهش آسیب پذیری کارتهای هوشمند. رتبه بندی به کمک آزمون ناپارمتریک فریدمن صورت گرفته است به این صورت که نخست به این مساله پرداخته شده است که آیا ما بین راهکارهای ارائه شده از نظر صاحب نظران ترجیح معناداری وجود دارد یا نه و در صورت معنادار شدن ترجیح رتبه بندی صورت گرفته است. این رتبه بندی ها در پنج سطح سخت افزاری، نرم افزاری، سیستم عامل، استاندارد و رتبه بندی کلی بوده است که نتیجه حاصل ارائه مدل راهکارهای کاهش آسیب پذیری کارتهای هوشمند بوده است.

۴-یافته‌های پژوهش و چارچوب پیشنهادی

یافته های پژوهش در سه بخش آسیب پذیریها، راهکارها و نهایتا چارچوب پیشنهادی در ادامه آورده شده است.

۴-۱- انواع آسیب پذیری‌های کارت های هوشمند

بعد از بررسی و تحلیل حملات مختلف بر روی کارتهای هوشمند و بررسی مقالات متعدد در خصوص آسیب پذیری های کارت هوشمند ، مهمترین منابع آسیب پذیری کارت های هوشمند (v)در دسته های ذیل شناسایی گردید:

V۱ عدم رعایت اصول خاص کارتهای هوشمند در طراحی تراشه های کارت هوشمند

V۲ عدم رعایت اصول رمز نگاری یا نوع الگوریتم های به کار رفته در کارت هوشمند

V۳ منابع تهیه کارتهای هوشمند

V۴ عدم وجود کارت هوشمند بومی و یا سامانه عامل بومی.
V۵ عدم کنترل کامل بر تراکنش های کارت هوشمند.
V۶ عدم رعایت اصول برنامه نویسی خاص کارتهای هوشمند

۴-۲- راهکارهای استخراج شده

برای رفع آسیب پذیری های استخراج شده راهکار های مختلفی در چهار حوزه اصلی کارتهای هوشمند یعنی سخت افزار ، نرم افزار، سامانه عامل و استاندارد به شرح ذیل استخراج شده است:

۴-۲-۱- راهکارهای حوزه سخت افزار

H۱ استفاده از ماژول چند لایه جهت کاربردهای مختلف
H۲ ایجاد یک مکانیزم امنیتی بومی منتشر نشده جهت برقراری امنیت کارت هوشمند
H۳ عدم امکان برقراری اتصال به باسهای درونی تراشه از بیرون از کارت
H۴ انتقال فناوری تولید و ساخت تراشه های کارت هوشمند در داخل کشور
H۵ عدم وابستگی به یک فراهم کننده ماژول
H۶ استفاده از ساختارهای میکرومتر در تولید تراشه
H۷ طراحی ویژه و جدا از روالهای مرسوم طراحی پردازنده و حافظه
H۸ قرار گرفتن حافظه ROM در لایه های میانی تراشه
H۹ استفاده از لایه فلزی برای زیر و روی تراشه جهت جلوگیری از اسکن شدن
H۱۰ استفاده از حسگر دما در کنار حافظه RAM
H۱۱ ایجاد درهم ریختگی نرم افزاری برای حافظه EEPROM
H۱۲ استفاده از الگوریتم رمز بومی جهت رمزگذاری فضای آدرس دهی
H۱۳ وجود حسگر نوری بر روی تراشه جهت تشخیص نفوذ فیزیکی
H۱۴ وجود مدار ناظر ولتاژ برای تراشه
H۱۵ وجود مدار ناظر فرکانس برای تراشه
H۱۶ درهم ریختگی منحصر به فرد برای باسهای درونی تراشه
H۱۷ استفاده از رگولاتورهای سریع جهت یکسای سازی جریان مصرفی
H۱۸ استفاده از مولد نویز مصنوعی جهت یک سان سازی جریان مصرفی
H۱۹ وجود مقاومت حسگر برای تنظیم جریان مصرفی
H۲۰ جلوگیری از اتصال سیمهای اضافی به ترمینالها با ایجاد دیافراگمهایی بر روی ترمینال
H۲۱ استفاده از حسگر های آشکارساز ولتاژ یا نور ناگهانی برای تشخیص مزاحمت های اضافی روی تراشه

۴-۲-۲- راهکارهای حوزه سامانه عامل

OS۱ وجود دانش فنی لازم بر روی سامانه عامل غیربومی انتخاب شده برای کارت هوشمند
OS۲ استفاده از پروتکل های تبادل اطلاعات بومی و امن
OS۳ استفاده از تکنیک امنیتی منتشر نشده و ویژه در توابع بومی شده سامانه عامل
OS۴ استفاده از دیواره آتش در ماشین های مجازی جاوا به منظور جلوگیری از دسترسی غیر مجاز
OS۵ استفاده از زبان برنامه نویسی امن در فرایند تولید سامانه عامل و نرم افزار
OS۶ سامانه عامل جاوا و MULTOS به عنوان سامانه عامل متن باز پیشنهاد می گردد
OS۷ استفاده از زبان میانی امن برای ترجمه زبان برنامه نویسی استفاده شود
OS۸ دسترسی به منابع کارت هوشمند به جز در موارد خاص محدود شده و در مستندات مشخص گردد
OS۹ ارزیابی کارت در سطوح مختلف
OS۱۰ ثبت امن حالات و شرایط فعلی عملکردی نرم افزار کارت
OS۱۱ استفاده از تصدیق اصالت دوطرفه برای کارت و پایانه
OS۱۲ محدودیت برای حداکثر میزان تراکنش های برون خط
OS۱۳ استفاده از توابع HMAC در مواردی که به محرمانگی نیازی نیست
OS۱۴ استفاده از یک سامانه عامل بومی یا بومی سازی سامانه عامل های موجود
OS۱۵ غیر فعال سازی کارت هوشمند در انتهای چرخه حیات

۴-۲-۳- راهکارهای حوزه نرم افزار

SS۱ استفاده از منابع داخل کارت به صورت بهینه (چند کاربردی بودن کارت)
SS۲ استفاده از روشهای نرم افزاری جهت جلوگیری از حمله کانال جانبی
SS۳ استفاده از تمهیدات و سازوکار های مختلف امنیتی متناسب با کاربرد کارت (PIN و رمز دوم)

SS۴ عدم انتشار روتین دستورات و کلاس دستورالعمل های درون نرم افزار کارت
SS۵ مقایسه تمامی ارقام PIN به صورت یکباره
SS۶ استفاده از مکانیزم های رمز و احراز اصالت غیروابسته به زمان پردازش داده ها و کلید
SS۷ استفاده از الگوریتم های رمز نگاری عاری از نویز
SS۸ وجود فلوچارت قوی به همراه روتین های تعیین شده برای هر شرط در برنامه و نرم افزار
SS۹ رمز کردن ارتباطات حساس کارت با ترمینال
SS۱۰ مخفی سازی ثبات ها و شمارنده های نشانگر اجرای برنامه
SS۱۱ ترتیب قرار گرفتن مناسب دستورالعمل در EEPROM

۴-۲-۴- راهکارهای حوزه استاندارد

sts۱ عدم استفاده از سیگنال VPP برای نوشتن بر روی حافظه کارت
sts۲ اجرای فرمان های مجاز و تعریف شده بر اساس دیاگرام حالت محدود
sts۳ استفاده از الگوریتم بومی برای رمزنگاری نامتقارن
sts۴ استفاده از الگوریتم درهم سازی (Hash) بومی
sts۵ محاسبه Checksum رمزنگاری به صورت بومی
sts۶ استفاده از قالب بومی برای ذخیره سازی اطلاعات بیومتریک
sts۷ استفاده از مکانیسم های تصدیق اصالت بومی
sts۸ گواهی حداقل EAL 3+ جهت استفاده از کارت هوشمند
sts۹ استفاده از الگوریتم مولد اعداد تصادفی اختصاصی
sts۱۰ استفاده از کارکنانی که از لحاظ امنیتی مورد تایید باشند
sts۱۱ استفاده از کارت با ماسک سخت و یا کارت اختصاصی
sts۱۲ عدم استفاده از کارت با قابلیت تنظیم مجدد
sts۱۳ استفاده از هولوگرام، متون حکاکی شده، نوار مغناطیسی و بیومتریک به منظور بالابردن امنیت بدنه کارت
sts۱۴ استفاده از کاربردها و نیازهای امنیتی مشابه یک کارت

۴-۲-۵- چارچوب کاهش آسیب پذیری

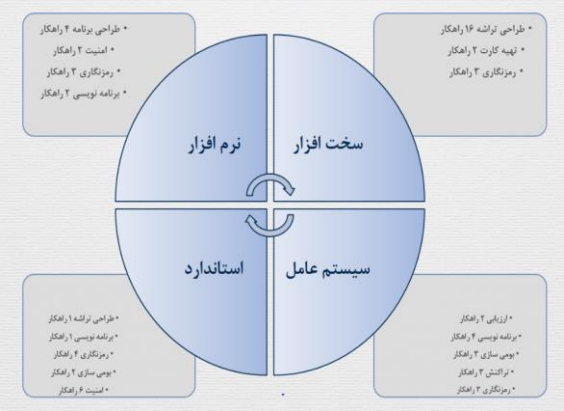
به‌منظور ارائه چارچوب راهکارهای کاهش آسیب پذیری کارتهای هوشمند با توجه به تجزیه تحلیل صورت گرفته، دسته بندی راهکارها ذیل چهار حوزه سخت افزاری، نرم افزاری، سامانه عامل و استاندارد پیشنهاد می شود. در جدول (۳) راهکارهای کاهش آسیب پذیری کارتهای هوشمند با احتساب چهار حوزه سخت افزاری، نرم افزاری، سامانه عامل و استاندارد ارائه شده است.
در شکل (۴) چارچوب پیشنهادی برای کاهش آسیب پذیری کارتهای هوشمند ارائه شده است.
این چارچوب بر اساس چهار بعد سخت افزار، نرم افزار، سامانه عامل و استاندارد در کارتهای هوشمند می باشد. در هر کدام از

جدول (۳): مهمترین راهکارهای کاهش آسیب پذیری کارتهای هوشمند

حوزه سخت افزاری	حوزه نرم افزاری	حوزه سامانه عامل	حوزه استاندارد
استفاده از الگوریتم رمز بومی جهت رمزگذاری فضای آدرس دهی	وجود دانش فنی لازم بر روی سامانه عامل غیربومی انتخاب شده برای کارت هوشمند	رمز کردن ارتباطات حساس کارت با ترمینال	استفاده از الگوریتم درهم سازی (Hash) بومی
انتقال فناوری تولید و ساخت تراشه های کارت هوشمند در داخل کشور	استفاده از پروتکل های تبادل اطلاعات بومی و امن	استفاده از تمهیدات و مکانیزم های مختلف امنیتی متناسب با کاربرد کارت (PIN و رمز دوم)	استفاده از کارکنانی که از لحاظ امنیتی مورد تایید باشند
استفاده از حسگر های آشکارساز ولتاژ یا نور ناگهانی برای تشخیص مزاحمت های اضافی روی تراشه	استفاده از تکنیک امنیتی منتشر نشده و ویژه در توابع بومی شده سامانه عامل	استفاده از مکانیزم های رمز و احراز اصالت غیروابسته به زمان پردازش داده ها و کلید	محاسبه Checksum رمزنگاری به صورت بومی
جلوگیری از اتصال سیمهای اضافی به ترمینالها با ایجاد دیافراگمهایی بر روی ترمینال	استفاده از زبان برنامه نویسی امن در فرایند تولید سامانه عامل و نرم افزار	استفاده از الگوریتم های رمز نگاری عاری از نویز	استفاده از قالب بومی برای ذخیره سازی اطلاعات بیومتریک
عدم امکان برقراری اتصال به باسهای درونی تراشه از بیرون از کارت	استفاده از تصدیق اصالت دوطرفه برای کارت و پایانه	عدم انتشار روتین دستورات و کلاس دستورالعمل های درون نرم افزار کارت	عدم استفاده از کارت با قابلیت تنظیم مجدد

حوزه ها راهکارها دسته بندی شده و تعداد راهکارها در هر دسته به صورت یک عدد در کنار دسته بندی آن ذکر شده است.

- حوزه سخت افزار به سه دسته طراحی تراشه، تهیه کارت، رمز نگاری تقسیم بندی شده است.
- حوزه نرم افزار به چهار دسته طراحی برنامه، امنیت، رمز نگاری، برنامه نویسی ذیل تقسیم بندی شده است.
- حوزه سامانه عامل به پنج دسته ارزیابی، برنامه نویسی، بومی سازی، تراکنش، رمزنگاری تقسیم بندی شده است.
- حوزه استاندارد به پنج دسته طراحی تراشه، برنامه نویسی، رمز نگاری، بومی سازی، امنیت تقسیم بندی شده است.



شکل (۴): چارچوب راهکارهای کاهش آسیب پذیری کارتهای هوشمند

۵- اعتبار سنجی چارچوب و راهکارهای پیشنهادی

همانطور که در روش تحقیق عنوان شد، مطالعات موردی و آزمون ناپارامتریک فریدمن برای اعتبارسنجی چارچوب راهکارهای پیشنهادی استفاده شد، این صورت که نخست به این مساله پرداخته شده است که آیا ما بین راهکارهای ارائه شده از نظر صاحب نظران ترجیح معناداری وجود دارد یا نه و در صورت معنادار شدن ترجیح رتبه بندی صورت گرفته است.

جدول(۴): نتایج آزمون فریدمن در معناداری وجود ترجیح راهکارهای حوزه سخت افزاری، نرم افزاری، سیستم عامل و استاندارد

عنوان	حوزه سخت افزار	حوزه نرم افزار	حوزه سیستم عامل	حوزه استاندارد
تعداد (N)	۲۱	۱۵	۱۱	۱۴
Chi-Square	۷۳/۱۳۰	۳۲/۸۵۷	۱۸/۶۴۰	۲۵/۱۷۴
درجه آزادی	۲۰	۱۴	۱۰	۱۳
P-value	۰/۰۰۰	۰/۰۰۳	۰/۰۴۵	۰/۰۲۲
عنوان	مقدار	۱۵	۱۱	۱۴
تعداد (N)	۱۵	۳۲/۸۵۷	۱۸/۶۴۰	۲۵/۱۷۴
Chi-Square	۳۲/۸۵۷	۱۴	۱۰	۱۳
درجه آزادی	۱۴	۰/۰۰۳	۰/۰۴۵	۰/۰۲۲
P-value	۰/۰۰۳	۱۵	۱۱	۱۴

نتایج آزمون فریدمن در راهکارهای ابعاد چهارگانه، در جدول (۴) نمایش داده شده است. در این جدول مشاهده می شود که مقدار P-value آزمون صفر درصد می باشد و این مقدار کوچکتر از سطح معنی داری ۵ درصدی است پس می توان نتیجه گرفت بین راهکارهای کاهش آسیب پذیری کارتهای هوشمند در هر یک از این حوزه ها اولویت وجود دارد. این اولویت یا ترجیح بر اساس نتایج آزمون، رتبه بندی شده و راهکارهای این حوزه به ترتیب این رتبه بندی در چارچوب پیشنهادی درج شده است.

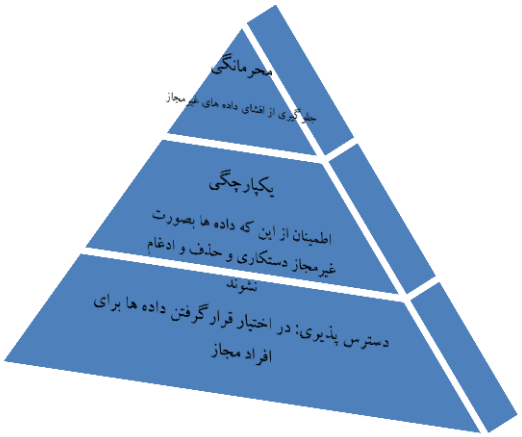
۶- نتیجه گیری

مقوله امنیت برای دستیابی به سه عامل مهم است که با یک دیگر مثلث امنیتی را تشکیل می دهند. این عوامل عبارتند از محرمانگی[1] ، یکپارچگی[2] و در نهایت دسترس پذیری[3]. این سه عامل (مثلث امنیت CIA) اصول اساسی امنیت اطلاعات را تشکیل می دهند. بگونه ای که تمامی تمهیدات لازمی که برای امنیت اتخاذ میشود و یا تجهیزاتی که ساخته می شوند، همگی ناشی از نیاز به اعمال این سه پارامتر در محیط های نگهداری و تبادل اطلاعات است.

نتایج این پژوهش به مجموعه ای از ۶۱ راهکار در چهار حوزه سخت افزار، نرم افزار، سامانه عامل و استانداردهای کارتهای هوشمند منتج شده است. با رعایت این راهکارها می توان امیدوار بود که آسیب پذیریهای کارتهای هوشمند به حداقل برسد با این وجود باید متوجه بود که امنیت هیچ موقع صد درصد نمی باشد و همیشه باید تعادلی بین سه حوزه محرمانگی ، یکپارچگی و دسترسی پذیری به وجود آورد.

امنیت کارت هوشمند بر چهار پایه اصلی سخت افزار ، نرم افزار ، سامانه عامل و استاندارد استوار می باشد . امنیت مناسب زمانی ارائه خواهد شد که به تمامی این چهار رکن اصلی کارت هوشمند توجه گردد. بر همین اساس می بایست مطابق نوع کاربری که از کارت هوشمند مورد نیاز می باشد و همچنین فاکتور مهم هزینه فایده، راهکارهای مناسبی انتخاب نمود. در غیر این صورت راهکارهایی که به نوعی تمامی این چهار رکن را شامل نگردد عملا ارائه کننده امنیت در کارتهای هوشمند نمی باشند.

همچنین، مطمئنا هر راهکاری برای بالا بردن امنیت کارتهای هوشمند استفاده شود باید سه ضلع مثلث امنیت CIA را در نظر گرفت (شکل ۵).



شکل(۵): مدل امنیت CIA [۱۱]

[1] Confidentiality
[2] Integrity
[3] Availability

به عنوان نمونه کاربردهایی که تبادل اطلاعات و یا ذخیره سازی اطلاعات حساس برای کارت در نظر گرفته می شود، می‌بایست با صرف هزینه بیشتر امنیت نسبی را برای این نوع کارت تأمین کرد. اما برای امور تردد نیاز به هزینه بالایی برای امنیت کارت هوشمند نمی باشد.

ضمنا، روند فناوری عملا بحث کارتهای هوشمند را به سمت تراشه های کاشتنی هوشمند، احراز هویت زیست‌سنجی و هوش مصنوعی سوق داده است. لذا مفهوم کارت جای خود را به ابزارهای نوین خواهد داد که واجد ویژگی تعبیه شده انسانی خواهد بود. منظور، جزیی از بدن یا تراشه ای متصل به بدن انسان است. تا آن زمان و در کشور ما هنوز روند استفاده از فناوریهای فعلی کارت هوشمند جریان دارد و لذا تمهیدات امنیتی ارایه شده در این پژوهش می تواند پیش گیرنده و ارتقاء دهنده کاهش آسیب پذیریهای کارتهای هوشمند باشد.

۷- مراجع

[1] J. D. Twizeyimana and A. Andersson, "The public value of E-Government–A literature review," Government information quarterly, vol. 36, no. 2, pp. 167-178, 2019.

[2] A. Mohtarami, "Investigating the relationship between information technology and innovation capability of economies: towards a virtual national innovation system", International Journal of Technological Learning, Innovation and Development, vol. 9, no. 3, pp. 230-249, 2017.

[3] S. R. Chohan, and G. Hu, "Strengthening digital inclusion through e-government: Cohesive ICT training programs to intensify digital competency. Information technology for development", vol. 28, no.1,pp.16-38, 2022.

[4] K. E. Markantonakis, and M. Konstantinos, "Smarty Cards/Tokens Security and Applications," University of London International Academy, vol. I, no. 5, pp. 55-60, ۲۰۰۷.

[5] Hendry, Mike. "Multi-application smart cards: technology and applications". Cambridge university press, 2007.

[6] J. I. den Hartog, and E. P. de Vink, "Virtual Analysis and Reduction of Side-Channel Vulnerabilities of Smartcards," Springer, vol. i, no. 14, p. 26, 2005.

[7] Rohatgi, Paul Kocher, Joshua Jaffe, Benjamin Jun, Pankaj, "Introduction to differential power analysis," Springer, vol. 1, no. 5, pp. 5-27, 2010.

[8] M. Neve, E. Peeters, D. Samyde, and J. Quisquater, "Memories: a survey of their secure uses in smart cards," ieee, vol. i, no. 13, pp. 1-10, 2003.

[9] L. Rivie`re, Julien Bringer, T. Ha Le, and H. Chabanne, "A Novel Simulation Approach for Fault Injection Resistance Evaluation on Smart cards," IEEE, vol. i, no. 12, pp. 1-8, 2015.

[10] B. Fouladi, Konstantinos Markantonakis and Keith Mayes, "Vulnerability Analysis of a Commercial .NET Smart Card," ieee, vol. II, no. 12, pp. 1-15, 2014.

[11] Shostack, Adam. Threat modeling: Designing for security. John Wiley & Sons, 2014.

[12] Mahanta, Hridoy Jyoti, Abul Kalam Azad, and Ajoy Kumar Khan. "Power analysis attack: A vulnerability to smart card security." In 2015 International Conference on Signal Processing and Communication Engineering Systems, pp. 506-510. IEEE, 2015.

[13] P. Hsieh-Tsen, H. W. Yang, and M. S. Hwang, "An enhanced secure smart card-based password authentication scheme." Int. J. Netw. Secur. 22, no. 2. pp. 358-363, 2020.

[14] H. Zhang and M. Li, "Security Vulnerabilities of An Remote Password Authentication Scheme with Smart Card," IEEE, vol. 3, no. 4, pp. 1-4, 2010.

[14] V. Singh, P. Dahiya, and S. Singh, "Smart Card Based Password Authentication and User Anonymity Scheme using ECC and Steganography," ieee, vol. II, no. 6, pp. 1-8, 2014.

[15]M. A. Nor Fazlina, N. Z. Abd Hashim, and H. Chizari, "Security Issues in ATM Smart Card Technology," International Journal of Mathematics and Computational Science, vol. I, no. 4, pp. 199-205, 2015.

[۱۶] کاظمی آشتیانی، رسول، خادم، بهروز، یک پروتکل احراز اصالت دوسویه در کارت هوشمند، نشریه علمی پدافند غیرعامل، دوره ۳، شماره ۳، شهریور ۱۳۹۱.

[۱۷] ترابی، میترا، شهیدی نژاد، علی، یک طبقه‌بندی از حملات تزریق SQL و روش‌های دفاع از این حملات در پدافند غیرعامل، نشریه علمی پدافند غیرعامل، دوره ۹، شماره ۳، صص ۱۱۷-۱۰۱، شهریور ۱۳۹۷. DOR: 20.1001.1.20086849.1397.9.3.10.9