الزامات به‌کارگیری فنآوری RFID[1] در ارتقای سطح امنیت اطلاعات طبقه‌بندی‌شده با تأکید بر پدافند غیرعامل (مطالعه موردی وزارت دفاع و پشتیبانی نیروهای نیروهای مسلح)

تاریخ دریافت: ۱۳۹۳/۱۱/۱۰
تاریخ تأیید: ۱۳۹۳/۱۲/۲۰

مجید اصغرزاده[2]
مهران ترحمی[3]
رضا جوادی[4]

چکیده

استفاده از فناوری‌های کنترلی نوین ازجمله RFID در زمینه حفاظت از دارایی‌های مهم و حساس، مستلزم توجه جدی به رفع نقاط آسیب‌پذیر فیزیکی و غیرفیزیکی (سایبری، مخابراتی و...) مترتب از به‌کارگیری این‌گونه فنآوری‌ها است.

هدف از نوشتار حاضر «احصای الزامات به‌کارگیری این فنآوری در راستای ارتقای سطح امنیت اطلاعات طبقه‌بندی‌شده وزارت دفاع و پشتیبانی نیروهای مسلح» است. در همین راستا این سؤال مطرح شد که «الزامات ارتقای سطح امنیت اطلاعات طبقه‌بندی‌شده ودجا با به‌کارگیری فنآوری RFID با تأکید بر پدافند غیرعامل کدامند؟» و برای پاسخ‌گویی به آن با این فرض که «الزامات ارتقای سطح امنیت اطلاعات طبقه‌بندی‌شده ودجا با استفاده از این فناوری مذکور عبارتند از الزامات امنیت چرخه حیات اطلاعات، الزامات مربوط به نیروی انسانی کاربر فناوری و الزامات امنیت زیرساخت این فنآوری» طرح گردید. بدین منظور ضمن انجام مصاحبه از پرسش‌نامه محقق ساخته ۳۵ سؤالی که در طیف لیکرت طراحی شده بود، استفاده گردید و با بهره‌گیری از روش توصیفی- پیمایشی، داده‌های جمع‌آوری‌شده از طریق شیوه‌های آمار توصیفی و استنباطی مورد تجزیه‌وتحلیل قرار گرفتند. در پایان پژوهش، با توجه به تأیید فرضیهٔ اصلی، پیشنهادهای کاربردی برای ارتقای امنیت این فناوری و اطلاعات مرتبط با آن در قالب الزامات امنیت چرخهٔ حیات اطلاعات، الزامات مربوط به نیروی انسانی کاربر این فناوری و الزامات امنیت زیرساخت ارائه گردیده است.

کلیدواژه‌ها: *فنآوری RFID، پدافند غیرعامل، امنیت اطلاعات، طبقه‌بندی اطلاعات.*

1. Radio Frequency Identification Direction

۲- استادیار روانشناسی تربیتی دانشکده علوم و فنون فارابی (Masgharzadeh22@gmail.com)
۳- دانشجوی دکتری مهندسی الکترونیک دانشگاه صنعتی شریف (Tarahomi@ce.sharif.ir)
۴- کارشناسی ارشد پدافند غیرعامل گرایش امنیت ملی دانشکده علوم و فنون فارابی (نویسنده مسئول) (Hrj50@payam mail.ir)

مقدمه

پدافند غیرعامل به‌عنوان یکی از راهبردهای دفاعی و غیرنظامی در حفظ و حراست از زیرساخت‌ها و دارایی‌های حیاتی و حساس از دیرباز در کشورهای پیشرفته مورد توجه قرار گرفته و کشورهای توسعه‌نیافته یا درحال‌توسعه نیز طی سال‌های اخیر توجه به این موضوع کلیدی را به شیوه‌های مختلف در سیاست‌های کلان و راهبردی خود لحاظ نموده‌اند. قابلیت‌های منحصربه‌فرد پدافند غیرعامل در تدوین سازوکارها و الزامات امنیتی با استفاده از شیوه‌ها و ابزارهای نوین توانسته است جایگاه ویژه‌ای را در حوزه‌های مختلف ازجمله در زمینه تأمین و ارتقای امنیت تجهیزات دفاعی و نظامی به خود اختصاص دهد. در سازمان‌های دارای اسناد و مدارک و تجهیزات حاوی اطلاعات طبقه‌بندی‌شده از جمله ودجا استفاده از روش‌های سنتی پاسخگوی رفع معضلات امنیتی در کاهش آسیب‌پذیری‌های حوزهٔ اسناد و اطلاعات نخواهد بود و باید این امکان با بررسی روش‌های نوین و بهره‌گیری از فنآوری‌ها و سامانه‌های نوظهور به‌ویژه فنآوری شناسایی مبتنی بر امواج رادیویی RFID فراهم گردد.

فناوری RFID نیز به دلیل بهره‌گیری از بستر رادیویی برای تبادل اطلاعات و همچنین استفاده از سایر بسترهای الکترونیکی و مخابراتی در راستای کاربری‌های خاص همواره تهدیدهای بالفعل و بالقوه‌ای را به‌همراه دارد.

بیان مسئله

امروزه اگرچه اطلاعات از ماهیت و شکل گذشته خود در قالب‌های مختلف ازجمله دست‌نوشته‌ها و اسناد مکتوب گذر نموده و ماهیت الکترونیکی و رایانه‌ای گرفته است، لکن ماهیت فیزیکی آن در مقطع فعلی نیز همچنان ادامه داشته و ابزارهای تولید، تبادل و نگهداری اطلاعات امروزه نیز در قالب تجهیزات مختلف از جمله حافظه‌های قابل‌حمل، گوشی‌های تلفن همراه، فلش مموری‌ها، لوح‌های فشرده، رایانه‌های قابل‌حمل، تبلت‌ها و دیگر ابزارهای ذخیره‌ساز اطلاعات در جایگاه اطلاع‌رسانی و نگهداری اطلاعات به ایفای نقش می‌پردازند.

ازاین‌رو علاوه بر اهمیت حفظ اطلاعات موجود در شبکه‌های رایانه‌ای که در موضوع امنیت فاوا بدان پرداخته می‌شود، امنیت فیزیکی این ابزارها و تجهیزات نیز از اهمیت ویژه‌ای برخوردار بوده و ارتقای امنیت آن‌ها از طرق مختلف به‌ویژه سازوکارهای حفاظتی و کارکردهای پدافند غیرعامل از اهمیت بسزایی برخوردار است.

وزارت دفاع به‌عنوان یکی از حساس‌ترین مراکز تولید، تبادل و نگهداری اطلاعات طبقه‌بندی‌شده با دارا بودن حجم قابل‌توجهی از اسناد و تجهیزات اشاره‌شده ازجمله رایانه همراه، فلش مموری، لوح‌های فشرده و سایر مدارک و تجهیزات همواره در معرض بروز

تهدیدهای امنیتی مترتب بر این دارایی‌های ارزشمند قرار داشته است. ازاین‌رو در این تحقیق سعی خواهد شد ضمن احصای نقاط آسیب‌پذیر این حوزه، الزامات مؤثر در ارتقای سطح امنیت این فناوری و مدارک و تجهیزات مورداستفاده به‌عنوان حامل شناسهٔ را تدوین و پیشنهاد نمود.

اهمیت و ضرورت

از اهمیت تحقیق انجام‌شده می‌توان به این نکته اشاره نمود که با توجه به نقاط آسیب‌پذیر سامانه RFID، تدوین الزامات به‌کارگیری آن می‌تواند به‌عنوان یک مرجع و الگوی امنیتی برای استفاده از این فنآوری و در راستای امن‌سازی فرآیند نصب، بهره‌برداری، کاربری و درمجموع بهره‌برداری مطلوب و حداکثری از کارکردهای امنیتی آن درزمینهٔ حفاظت از اقلام و تجهیزات و اسناد حاوی اطلاعات طبقه‌بندی‌شده در مراکز نظامی و دفاعی بهره‌گیری نمود.

از منظر ضرورت تحقیق نیز می‌توان بر این موضوع تأکید نمود که با توجه به تغییر رویکرد اقدام‌های حفاظتی به‌سمت حوزه‌های فنآوری اطلاعات، نبود تدوین الزامات حفاظتی در ابعاد مختلف به‌کارگیری این سامانه، موجب تمرکز بر حوزهٔ فاوا شده و سایر نقاط آسیب‌پذیر مرتبط با این سامانه ازجمله دسترسی‌های فیزیکی به اجزا و اقلام حامل شناسهٔ RFID از طریق کاربران موردتوجه جدی قرار نگیرد.

هدف، سؤال و فرضیه

هدف این مقاله «آشنایی با الزامات این فنآوری در ارتقای سطح امنیت اطلاعات طبقه‌بندی‌شده ودجا» است. سؤال اساسی نیز این است که «الزامات ارتقای سطح امنیت اطلاعات طبقه‌بندی‌شده ودجا با به‌کارگیری این فنآوری کدامند؟» فرض هم بر این بنا شده که «الزامات ارتقای سطح امنیت اطلاعات طبقه‌بندی‌شده ودجا با استفاده از فنآوریRFID عبارتند از امنیت چرخهٔ حیات اطلاعات به‌وسیله فنآوری مذکور، نیروی انسانی بعنوان کاربر آن و نیز امنیت زیرساخت این فنآوری» محسوب می‌گردند.

پیشینه

تاکنون در خصوص موضوع مطالعهٔ جامع و ویژه‌ای انجام نگرفته، لیکن در ابعاد مختلف تحقیق مطالعه‌ای به‌صورت تخصصی و بیشتر در زمینه‌های فنی فنآوری RFID و همچنین پدافند غیرعامل انجام شده است که از مهم‌ترین آن‌ها می‌توان به مقاله جان‌نثاری لادانی و همکاران (۱۳۸۶) با عنوان «خطرهای امنیتی سامانه‌های RFID» اشاره نمود که در آن ضمن معرفی این فنآوری و قابلیت‌های آن، مشکلات امنیتی این فنآوری و اجزای آن ازجمله خواندن تگ‌های غیرمجاز، استراق سمع، ردیابی، تصادف تگ‌ها، ویروس و کرم‌ها را مورد بررسی قرار داده و راه‌حل‌هایی برای رفع این مشکلات ارائه نموده‌اند.

همچنین سلیمانی (۱۳۸۵) در مقاله‌ای با عنوان «چالش‌های RFID بر شبکه» علاوه بر پرداختن به برخی گرایش‌های تحقیقاتی جدید در رابطه با آن، تأثیر ورود این فناوری به قلمرو شبکه و مواردی که هر رویکرد ارائه شده درزمینهٔ استفاده از RFID در شبکه باید موردنظر داشته باشد، را بیان نموده است.

بررسی پژوهش‌های مذکور بیانگر این است که در زمینهٔ این فنآوری، نقاط آسیب‌پذیر و راه‌کارهای رفع آن‌ها از همه ابعاد به‌ویژه اجزای سامانه و کاربران تبیین نگردیده و فقط به آسیب‌پذیری‌ها و تهدیدهای نوین (سایبری و مخابراتی) این فنآوری اشاره شده است. بنابراین منابع اشاره شده بخشی از مطالعهٔ محقق در زمینه موضوع مورد تحقیق بوده که هرکدام به‌نوعی بخشی از ابعاد مختلف تحقیق را در بر گرفته است. این منابع به‌تنهایی پاسخ‌گوی سؤال‌های مطرح‌شده در این تحقیق نبوده و در نوشتار حاضر سعی خواهد شد الزامات به‌کارگیری این فناوری در راستای ارتقای امنیت اطلاعات موردبررسی و مطالعه قرار گیرد.

مبانی نظری و مفاهیم

پدافند غیرعامل: در بند اول سیاست‌های کلی نظام در خصوص پدافند غیرعامل که به تأیید مقام معظم رهبری رسیده است، تعریف پدافند غیرعامل به شرح زیر است:

«پدافند غیرعامل عبارت است از مجموعهٔ اقدام‌های غیرمسلحانه‌ای که باعث افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و آسانی مدیریت بحران در مقابل تهدیدها و اقدام‌های نظامی می‌گردد» (اسکندری،۱۳۹۱:۱۷).

شاخصه‌های اصلی پدافند غیرعامل: پدافند غیرعامل از شاخصه‌های اصلی بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، افزایش پایداری ملی و آسانی مدیریت بحران برخوردار است (جلالی،۱۳۹۱:۸۰). کارکردهای کلی پدافند غیرعامل: پدافند غیرعامل درمجموع از کارکردهای زیر برخوردار است.

۱- حفاظت از جان مردم؛
۲- حفاظت از زیرساخت‌های حیاتی؛
۳- استمرار خدمات ضروری؛
۴- حفاظت از تأسیسات و تجهیزات نادر؛
۵- پایدارسازی مدیریت عالی کشور؛
۶- حفاظت سایبری از کشور؛
۷- تأمین نیازهای مردم؛
۸- تداوم اداره مردم (جلالی،۱۳۹۰:۱).

اصول پدافند غیرعامل: اصول پدافند غیرعامل مجموعهٔ اقدام‌های بنیادی و زیربنایی است که در صورت به‌کارگیری آن‌ها می‌توان به اهداف پدافند غیرعامل از قبیل تقلیل خسارت‌ها و صدمه‌ها، کاهش قابلیت و توانایی سامانه‌های شناسایی اهداف، هدف‌یابی و دقت هدف‌گیری تسلیحات آفندی دشمن و تحمیل هزینه بیشتر به وی نائل گردید. پدافند غیرعامل شامل شانزده اصل است که اصل شانزدهم آن با عنوان «حفاظت اطلاعات سامانه‌های حیاتی و مهم» شامل موارد زیر است:

۱- حفاظت و حراست از کلیه اسناد، مدارک، مطالب، نقشه‌ها و... مراکز حیاتی، حساس و مهم.

۲- ایجاد اطمینان از نبود نشت اطلاعات سامانه‌های حیاتی و مهم.

۳- افزایش دانش و ایجاد انگیزه برای کارکنان مرتبط در حفاظت از اطلاعات طبقه‌بندی‌شده.

۴- تفکیک اطلاعات با در نظر گرفتن قالب‌های مختلف (نظامی، سیاسی و...).

۵- حفظ اطلاعات در محدوده خارجی که جزئی از اطلاعات تاکتیکی است.

۶- ایجاد امنیت در ابعاد مختلف و حفظ اطلاعات خودی و جلوگیری از انتشار آن

پدافند غیرعامل در حفاظت اطلاعات سامانه‌های حیاتی و مهم: زیرمعیارهای اصل شانزدهم از اصول پدافند غیرعامل بر اقدام‌های حفاظتی لازم در ابعاد مختلف حفاظتی تأکید دارد که این زیرمعیارها از کارکردهای متفاوتی در سطح نیروهای مسلح برخوردار بوده و به‌ویژه در بخش دفاع (وزارت دفاع و مراکز تابعه) از ارتباط مستقیم و دوسویه با کارکردهای حفاظت اطلاعات برخوردار است. با توجه به پوشش کلان اقدام‌های پدافندی در کلیه حوزه‌های مورد تهدید (سیاسی، اقتصادی، فرهنگی، دفاعی و...)، می‌توان کارکردهای حفاظت اطلاعات در حوزه‌های مقابله با آسیب‌پذیری‌های حفاظتی و امنیتی را جزئی از کارکردهای پدافند غیرعامل برشمرد (اسکندری،۱۳۹۱:۳۸).

اهداف پدافند غیرعامل در فضای سایبری: این اهداف شامل موارد زیر است:

۱-کاهش آسیب‌پذیری‌ها و ایمن‌سازی شبکهٔ فناوری اطلاعات و ارتباطات کشور؛

۲- افزایش بازدارندگی و تولید قدرت در حوزهٔ سایبری؛

۳- تداوم فعالیت‌های ضروری سایبری؛

۴- ارتقای پایداری زیرساخت‌های کشور در برابر تهدیدهای سایبری؛

۵- بومی‌سازی تولید نرم‌افزارهای اساسی و پایه؛

۶- آسانی مدیریت بحران در زیرساخت‌های کشور در تهدیدهای سایبری؛

۷- بومی‌سازی و تدوین الگو و مدل دفاع سایبری کشور(جلالی، ۱۳۹۱: ۱۳۱-۱۳۰).

امنیت اطلاعات: امنیت اطلاعات به حفاظت از اشکال مختلف داده‌ها، سرویس‌ها، سامانه‌ها و

ارتباطات در برابر خطرها گفته می‌شود (اکبرپور، ۱۳۹۱: ۹) و حفاظت اطلاعات همهٔ اقدام‌هایی است که به‌منظور حفظ و نگهداری تأسیسات، اسناد و مدارک، اخبار و اطلاعات، کارکنان، مخابرات و سایر موضوع‌های حیاتی کشور در برابر خطرهای ناشی از جاسوسی، براندازی، خرابکاری، سرقت و خطرهای طبیعی به‌عمل می‌آید و از دسترسی افراد غیرمجاز به موارد گفته‌شده جلوگیری می‌کند (ساحفاودجا، ۱۳۹۱: ۴).

در یک تعریف کلی و مرتبط با موضوع می‌توان گفت، «امنیت اطلاعات» به مجموعه‌ای از تدابیر، روش‌ها و ابزارهایی برای جلوگیری یا کاهش دسترسی و تغییرات غیرمجاز اشکال مختلف اطلاعات در نظام‌های نگهداری و تبادل سنتی و رایانه‌ای اطلاعات گفته می‌شود (کاظم پور،۱۲:۱۳۹۲).

اهداف پدافند غیرعامل از منظر اقدام‌های حفاظتی: برای انجام اقدام‌های حوزهٔ پدافند غیرعامل و همچنین اقدام‌های حفاظتی، چاره‌ای جز تعیین و تبیین اهداف قابل حفاظت نیست. ابتدا بایستی معین شود چه چیز باید موردحفاظت قرار گیرد و سپس به طرح‌ریزی و برنامه‌ریزی برای حفاظت از آن پرداخت. در این راستا به‌طورکلی می‌توان اجزای قابل حفاظت سازمان را به چهار رده زیر تقسیم نمود:

۱- کارکنان (سازمان)؛

۲- اماکن و تأسیسات؛

۳- ابزار و تجهیزات؛

۴- اخبار، اطلاعات، اسناد و مدارک (علوی فر، ۱۳۸۵: ۱۲۲).

تقسیم‌بندی اسناد و اطلاعات: اسناد و تجهیزات حاوی اطلاعات را به لحاظ ارزش حفاظتی و میزان مراقبتی که باید از آن‌ها به‌عمل آید، به دو دسته کلی می‌توان تقسیم‌بندی نمود که عبارتند از اسناد فاقد ارزش حفاظتی یا طبقه‌بندی[1] و اسناد دارای ارزش حفاظتی[2] (همان، ۳۵).

چهار نوع طبقه‌بندی در نیروهای مسلح ج.ا.ا وجود دارد که عبارتند از به‌کلی سری، سری، خیلی محرمانه و محرمانه (ستاد کل نیروهای مسلح، ۲۱:۱۳۷۵).

عوامل تهدیدکننده اسناد و اطلاعات: عواملی که (حفاظت) اسناد و اطلاعات را تهدید و آن را در معرض خطر قرار می‌دهند، به سه دسته کلی زیر تقسیم می‌شوند:

۱- عوامل محیطی؛ شامل: نور، دما، رطوبت، آلودگی و گردوغبار و ... ؛

۲- حوادث طبیعی؛ شامل: باران و سیل، زلزله، رعدوبرق، آتش‌سوزی‌ها و ... ؛

1. Unclassified document
2. Restricted document

۳- عوامل انسانی؛ شامل: عناصر وابسته به سازمان‌های اطلاعاتی حریف و گروه‌های معاند، سارقان، عوامل و احزاب سیاسی و... (علوی فر، ۱۳۸۵: ۲۴).

شیوه‌های حفاظت از اطلاعات: برای حفاظت از اسناد و اطلاعات (دارای ارزش حفاظتی) در سازمان‌ها و نهادهای اداری و اطلاعاتی از روش‌ها و سازوکارهای مختلفی استفاده می‌گردد که عمده‌ترین و مهم‌ترین آن‌ها عبارتند از:

۱- طبقه‌بندی (حفاظتی)[1]؛
۲- حیطه‌بندی[2]؛
۳- حفاظت فیزیکی؛
۴- بازرسی و کنترل؛
۵- امحا (باقریان، ۱۳۸۵: ۸۵).

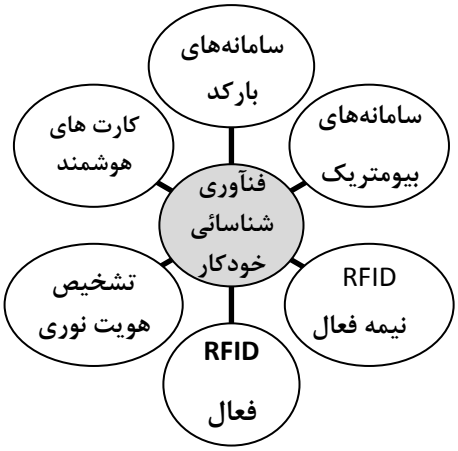
تهدیدهای فنآوری اطلاعات: تهدید در حوزهٔ فناوری اطلاعات می‌تواند وقایعی ازجمله دسترسی غیرمجاز، دست‌کاری، افشا یا خرابکاری روی دارایی‌های فنآوری اطلاعات را شامل شود. این تهدیدها در دو سطح مطرح هستند:

۱- مواردی که از جانب دشمنان و در خارج از مرزهای کشور برنامه‌ریزی و سازمان‌دهی می‌شوند و می‌توانند دارای بازه‌های زمانی کوتاه یا بلندمدت باشند.
۲- مواردی که در داخل و در حوزه‌های مختلف می‌توانند باعث ایجاد اخلال در سطوح مختلف فنآوری اطلاعات شده و تهدیدهای خارجی از ناحیهٔ دشمنان محسوب نمی‌شوند (ترحمی و همکاران، ۱۳۸۸: ۴۷).

فناوری‌های شناسایی خودکار: به‌طورکلی فنآوری شناسایی و جمع‌آوری خودکار داده‌ها (AIDC[3]) به روش‌هایی گفته می‌شوند که طی آن تجهیزات سخت‌افزاری و نرم‌افزاری قادر به دریافت و تشخیص داده‌ها بدون دخالت انسان می‌باشند (فدوی اردستانی، ۱۳۸۸: ۲۴).

سامانه‌های بیومتریک[4]، کارت‌های هوشمند[5]، تشخیص هویت از طریق نور (OCR[6])، بارکدها و بالاخره RFID نمونه‌هایی در این زمینه می‌باشند که در شکل شماره ۱ به آن‌ها اشاره شده است (Wyld, 2006:154-173).

1. Security Classification
2. Compartmention
3. Automatic Identification and Data Collection
4. Biometric Systems
5. Smart Card
6. Optical Character Recognition



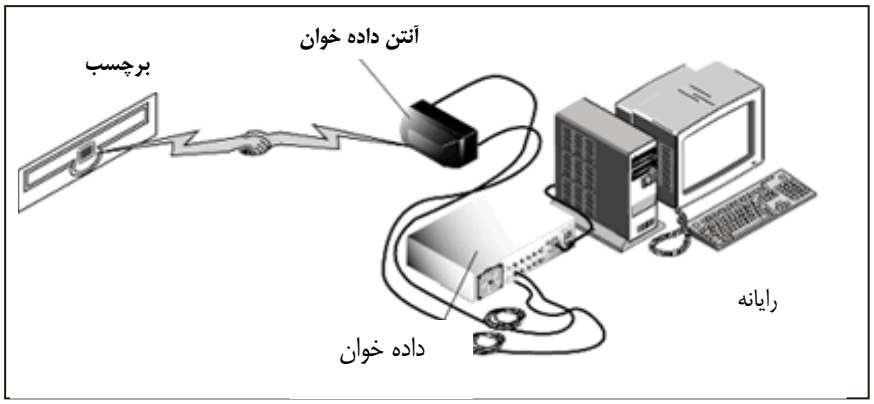
شکل شماره ۱. خانواده فنآوری‌های شناسایی خودکار.

تاریخچه پیدایش RFID: در سال ۱۹۴۶ لئون ترمین[1] ابزاری را برای دولت اتحاد جماهیر شوروی اختراع کرد که قادر بود امواج رادیویی ایجادشده ناشی از هرگونه وقایع و حوادث را در قالب اطلاعات صوتی به محل موردنظر انتقال دهد. این امواج صوتی با به حرکت درآوردن دیافراگمی که به یک دستگاه مرتعش کننده متصل بود، بازتاب امواج رادیویی را به زبان قابل‌فهم ترجمه می‌کرد. اگرچه این وسیله نوعی ابزار منفعل بود و توانایی‌های زیادی نداشت، توانست نام خود را به‌عنوان نخستین دستگاه مبتنی بر ساختار RFID به ثبت برساند. با وجود این برخی منابع اعلام کرده بودند که فنآوریRFID از سال ۱۹۲۰ در بین کارشناسان و متخصصان رواج پیدا کرد و در دهه ۱۹۶۰ تکمیل شد (دولت‌آبادی، ۱۳۸۶: ۷).

اجزای سامانهٔ RFID: یک سامانهٔ RFID که در شکل شماره ۲ مشخص است، از سه قسمت سخت‌افزاری[2]، میان‌افزاری[3] و نرم‌افزاری[4] تشکیل شده است (مقدسی و همکاران، ۱۳۸۸: ۳۸). سه قسمت کلی در برگیرنده اجزای اصلی سامانه RFID به شرح زیر می‌باشند:

۱- شناسه (برچسب)؛ ۲- بازخوان (داده خوان)؛ ۳- کنترل‌کننده (ستاد کل ن.م، ۱۳۹۱: ۵ و ۶).

1. Léon Theremin
2. Hardwar
3. Middleware
4. Software



شکل شماره ۲: اجزای سامانهٔ RFID .

برچسب: برچسب‌های RFID به‌منظور شناسایی و ذخیره‌سازی اطلاعات یک شی به آن متصل می‌شوند. هر برچسب از سه قسمت ریزتراشه[۱]، آنتن یا القاگر[۲] و منبع تغذیه[۳] تشکیل می‌گردد. ریزتراشه سیگنال دریافتی از دستگاه داده خوان را پردازش، ذخیره و تغییر می‌دهد و دوباره برای آن ارسال می‌نماید. آنتن، وظیفهٔ دریافت سیگنال از داده خوان و نیز تقویت سیگنال برگشتی از برچسب به داده خوان را دارد. همچنین برچسب‌ها می‌توانند با دریافت سیگنال از داده خوان انرژی موردنیاز خود را تأمین نمایند (مقدسی و همکاران، ۱۳۸۸: ۳۸).

برچسب‌ها بر اساس نحوهٔ تأمین انرژی مصرفی به سه دسته اصلی تقسیم می‌شوند:

- ✓ برچسب‌های فعال[۴]؛
- ✓ برچسب‌های نیمه فعال[۵]؛
- ✓ برچسب‌های غیرفعال[۶] (Potter,2005:17-18).

نقش برچسب در نشانه‌گذاری[۷] مدارک و تجهیزات: استفاده از برچسب RFID به‌عنوان یکی از روش‌های علامت‌گذاری مدارک، اقلام و تجهیزات قلمداد می‌شود که در آن با نصب برچسب RFID به اقلام اشاره شده می‌توان آنها را نشانی‌گذاری کرد و بر اساس ویژگی‌های این فناوری شناسایی و کنترل نمود. برخلاف روش‌های پنهان‌نگاری که اغلب اطلاعات محرمانه را در داده‌های متعارف پنهان می‌کنند و حتی اگر مهاجم از وجود چنین داده‌ای مطلع شود و آن را

1 - Microchip
2 - Inductor
3 - Power Source
4- Active Tag
5 - Semi-passive Tag
6 - Passive Tag
7 - watermark

دستکاری کند، به‌سادگی قابل‌تشخیص نخواهد بود، نشانه‌گذاری روشی است که از علامت‌گذاری‌های اضافی برای افزودن استحکام به داده‌ی محرمانه استفاده می‌کند و نابود کردن اطلاعات نشانه‌گذاری شده، حتی اگر از وجود داده‌های پنهان در آن خبر داشته باشیم ساده نیست (سلیمانی و همکاران، ۱۳۹۰: ۱۱۴).

داده خوان: داده خوان دستگاهی الکترونیکی است که سیگنال بازرسی[1] را تولید و دریافت می‌کند. سیگنال بازرسی یک سیگنال رادیوئی است که به‌وسیله آنتن یا آنتن‌هایی که به دستگاه داده خوان متصل شده‌اند، منتشر و دریافت می‌شود. می‌توان این‌طور بیان کرد که مجموعهٔ تشکیل‌دهندهٔ دستگاه داده خوان دو عمل دریافت و ارسال را انجام می‌دهند (مقدسی و همکاران، ۱۳۸۸: ۷۰).

کنترل‌کننده: کنترل‌کننده‌های RFID به‌منزلهٔ مغز متفکر یک سامانه عمل کرده و در هر شبکه، اغلب رایانهٔ شخصی یا ایستگاه کاری است که روی آن بانک اطلاعاتی یا سامانهٔ نرم‌افزاری اجرا شده است (یا شبکه‌ای از این ماشین‌ها)، بنابراین این بخش متشکل از سه بخش قسمت سخت‌افزار (رایانهٔ میزبان)، میان‌افزار و نرم‌افزار بوده و وظیفه مدیریت، پردازش و نمایش اطلاعات دریافتی از برچسب‌ها را که از طریق شبکه رمزخوان‌ها (بازخوان‌ها) جمع‌آوری می‌شوند بر عهده دارد (جلالیان، ۲۱:۱۳۹۰).

ویژگی‌های سامانهٔ RFID: این سامانه در راستای کنترل اموال و کالاهای خاص از قابلیت‌های مختلفی برخوردار است که اهم آن‌ها به شرح ذیل است:

۱- ایجاد فنس مجازی (رادیویی) و قابلیت کنترل دسترسی کارکنان، خودروها و اشیا (مانند لپ‌تاپ‌ها)؛

۲- ثبت لحظه‌ای فعالیت‌های افراد، خودروها و اشیای درون مناطق تعریف‌شده در سامانه؛

۳- امکان کنترل برخط حضور، آلارم و همهٔ اطلاعات روی نقشه؛

۴- قابلیت به‌کارگیری نقشه‌های دیجیتال، سامانه‌ی اطلاعات مکانی (GIS[2])؛

۵- تعریف قوانین و آلارم برای هر شی یا فرد؛

۶- قابلیت جابجایی آسان داده خوان‌ها برای سایت‌ها در حین ساخت بر حسب ضرورت؛

۷- قابلیت اتصال انواع حس‌گرهای مختلف به سامانهٔ نظیر حس‌گر دما، رطوبت، گاز و سایر عوامل شیمیایی (ایزایران،۷:۱۳۸۹).

از فناوری مذکور به دو صورت حلقهٔ بسته[1] و حلقهٔ باز[2] در طول فرآیندهای زنجیرهٔ تأمین

1 - Interrogation Signal
2 - Geographic Information System

استفاده می‌شود (امینی لاری و همکاران،۱۳۸۶:۴):

۱- RFID حلقه بسته: در سامانه‌های حلقه بسته، به‌کارگیری این فناوری و برچسب‌های آن فقط در فرآیندهای درون‌سازمانی مورد استفاده قرار می‌گیرد بدون هیچ ارتباطی با دنیای خارج از سازمان، مانند نگهداری محصول در انبار و در شعبه‌های مختلف سازمان. در ابتدا بیشتر شرکت‌ها به‌سمت به‌کارگیری فناوری حلقه بسته در سازمان خود بودند، به‌گونه‌ای که شرکت‌های بزرگی مانند وال مارت[3] و سونی[4] به‌سرعت به چنین سامانه‌هایی مجهز شدند.

۲- RFID حلقه باز: اشیائی که حاوی برچسب این فناوری در برنامه‌های حلقهٔ باز هستند، قادر هستند در کل زنجیرهٔ تأمین حرکت کنند به‌طوری‌که پردازش برچسب‌ها به‌وسیلهٔ تمامی شرکت‌ها و اعضای زنجیرهٔ تأمین میسر باشد. به‌عبارت‌دیگر در برنامه‌های حلقه باز هدف این است که اطلاعات مهم کالا که درون برچسب‌ها قرار دارند نه‌تنها در درون سازمان قابل استفاده باشد، بلکه در طول زنجیرهٔ تأمین بتوان در هر سازمان دیگری و حتی در طول ارسال کالا از این اطلاعات استفاده نمود.

کاربردهای اصلی سامانهٔ RFID:

۱- امکان نظارت و مدیریت بر اموال و افراد در محوطه‌های مختلف سازمان؛
۲- افزایش امنیت تجهیزات ارزشمند و گران‌قیمت مانند لپ‌تاپ‌ها، دستگاه‌های بیمارستانی و آزمایشگاهی، تجهیزات صنعتی و غیره؛
۳- کنترل تردد (نامحسوس) افراد در محوطه سازمان‌های بزرگ؛
۴- افزایش ایمنی افراد در محوطه‌های پرخطر؛
۵- مشاهده موقعیت تجهیزات و افراد و ردیابی افراد و کالاها در سازمان برای پیدا کردن موقعیت آن‌ها (ایزایران،۱۳۸۹:۳).

کاربرد در راستای حفاظت اسناد و اطلاعات: امکان ثبت اطلاعات کلی سند (ازجمله طبقه‌بندی) در هنگام نصب برچسب RFID به آن ازجمله ویژگی‌های بسیار مطلوب این فناوری است، ضمن اینکه تکمیل، اصلاح و به‌روزرسانی اطلاعات مربوط به محصول در طول حیات سند، امکانات دیگری را نیز برای کاربران فراهم می‌نماید که ازجمله این قابلیت‌ها در هر سه موضوع بالا می‌توان به موارد زیر اشاره نمود:

1 - Closed Loop
2 - Open Loop
3 - Wal-Mart
4 - Sony

۱- امکان ثبت طبقه‌بندی واقعی سند و ناممکن نمودن ایجاد تغییر در طبقه‌بندی، بدون مجوز مدیر سامانه؛
۲- امکان اطلاع از طبقه‌بندی سند بدون مراجعه به محتوای سند؛
۳- امکان آمارگیری از تعداد و تنوع طبقه‌بندی اسناد؛
۴- برنامه‌ریزی برای مجزا نمودن مکان نگهداری اسناد با طبقه‌بندی‌های یکسان؛
۵- فراهم نمودن امکان هشدار دادن سامانه در هنگام انقضای مدت‌زمان طبقه‌بندی سند برای تقلیل یا تغییر طبقه‌بندی سند؛
۶- امکان ایجاد حیطه‌بندی برای اسناد با دسته‌بندی‌های مختلف و ایجاد سامانهٔ هشدار در صورت تغییر حیطهٔ دسترسی؛
۷- فراهم نمودن امکان هشدار دادن سامانه در هنگام انقضاء مدت‌زمان حیات سند برای امحاء سند (جواهری، ۷۶:۱۳۸۷).

مباحث امنیتی RFID: یک فرد یا برچسب خوان هوشمند به‌راحتی می‌تواند محتوای برچسب‌ها، به‌عنوان مثال رمز منحصربه‌فرد محصول‌های الکترونیکی (EPC[1]) را خوانده یا تغییر دهد. با توجه به اینکه برچسب‌های آن از فواصل چند متری نیز قابل‌خواندن هستند، این عمل کار چندان دشواری به‌نظر نمی‌رسد و چون بسترش از نوع بی‌سیم است که باعث کاهش امنیت دسترسی به برچسب‌های آن می‌شود (برکتین، ۴:۱۳۸۵). برای پرداختن به مقولهٔ امنیت در به‌کارگیری این فنآوری لازم است نقاط آسیب‌پذیر این فنآوری و خدمات ناشی از بهره‌گیری آن را مورد بررسی قرار دهیم.

تهدیدهای معروف این فناوری: فنآوری RFID جمع‌آوری اطلاعات را در مورد مکان‌ها و عملیات مجزا به‌صورت خودکار انجام می‌دهد که این اطلاعات می‌تواند ازسوی افراد مختلف اعم از هکرها، حریفان و... مورد دسترسی و سو استفاده قرار گیرد. این تهدیدها بسته به نقاط آسیب‌پذیر سامانه ممکن است از طرف افراد مجاز (کاربر، مدیر سامانه و سایر افراد دارای دسترسی) یا از طریق افراد غیرمجاز و به طرق مختلف از جمله نفوذ و... اجزای سامانه یا اطلاعات را مورد هدف قرار دهد (عموزاد خلیلی، ۸:۱۳۸۶).

تعدادی از تهدیدهای رایج امنیتی آن عبارتند از:

الف. تهدیدهای فیزیکی: به‌طورمعمول برای انجام چنین حمله‌هایی، لازم است که برچسب‌ها به‌طور فیزیکی دست‌کاری شوند. بعضی از گونه‌های حملهٔ فیزیکی عبارتند از: هک کردن

1 - Electronic Product Code

اطلاعات با تابش اشعه، از بین بردن مادهٔ نگهداری کنندهٔ اطلاعات، در معرض رطوبت قراردادن، قطع ساعت زمانی برچسب و مواردی مانند این‌ها. برچسب‌های RFID در برابر چنین حمله‌هایی مقاومت کمی دارند (همان). تعداد زیادی از حمله‌های فیزیکی در دو نوع انجام می‌شوند، حملات غیر هجومی (تحلیل زمانی، قدرتی، نقاط ضعف عملکردی، فرکانس‌های کاری و تحلیل مسیر انتقال اطلاعات) و حملات هجومی (استفاده از ریز کاوشگر[1]، استفاده از مسیر انتقال اطلاعات برای استخراج داده‌ها با استفاده از میکروسکوپ لیزری). (جان‌نثاری لادانی، ۹:۱۳۸۶).

درهرصورت مهم‌ترین و اصلی‌ترین موضوع در فرآیند حمله‌های فیزیکی لزوم دسترسی فیزیکی به اجزا و تجهیزات سامانه RFID است که این موضوع می‌تواند از جانب کاربران یا نفوذگران صورت پذیرد، بنابراین لزوم کنترل دسترسی‌ها و نظارت بر اقدام‌ها و فرآیندهای دسترسی فیزیکی به سامانه و اجزای آن از اولویت بسیار بالایی برای رفع نقاط آسیب‌پذیر این حوزه برخوردار است.

ب. تهدیدهای غیرفیزیکی: این تهدید شامل تهدیدهای سایبری، شنود یا هر چیزی است که مستلزم دسترسی فیزیکی به برچسب‌ها و داده خوان‌ها نباشد. برخی از اهم این تهدیدها عبارتند از:

۱- ردیابی[2]: در این تهدید قرائت گرهای RFID در مکان‌های خاصی نصب می‌شوند تا هویت یک برچسب را ثبت نموده و ردیابی کنند (روهینا، ۱:۱۳۸۵).

۲- تجاوز به حریم خصوصی[3]: در این نوع تهدید هر فردی با داشتن یک برچسب خوان به‌راحتی می‌تواند کلیه اجناس و اشیای برچسب دار داخل حریم خصوصی شما (مانند خانه) را شناسایی نموده و در سر فرصت اقدام به سرقت آنها نماید (برکتین، ۵:۱۳۸۵).

۳- استراق سمع: در این روش خواندن اطلاعات برچسب‌ها ممکن است بدون اطلاع حامل برچسب انجام شود و می‌تواند از راه دور خوانده شود (روهینا، ۱:۱۳۸۵).

۴- دست‌کاری داده‌ها[4]: این نوع تهدید زمانی به وقوع می‌پیوندد که فرد غیرمجاز داده‌ها را خوانده، تغییر دهد یا چیزی را به آن اضافه و حذف نماید (برکتین، ۹:۱۳۸۵)

۵- حمله‌های پاسخ: حمله‌کنندگان می‌توانند با استفاده از رله RFID در هنگام جستجوی RFID از آن جلوگیری کنند و اطلاعات دیگری را ارسال نمایند (روهینا، ۲:۱۳۸۵).

1 - micro probing
2 - Follow an Active
3 - Aggression to Private limits
4 - Manipulating of Information

۶- آشکارسازی اطلاعات[1]: ساده‌ترین و درعین‌حال مهم‌ترین تهدیدی که برای سامانهٔ RFID وجود دارد، این است که یک فرد در یک محیط به‌راحتی برچسب‌های RFID را خوانده و آن‌ها را روی سامانهٔ ذخیره‌سازی، ذخیره نماید (برکتین، ۱۰:۱۳۸۵).

۷- ممانعت از ارائهٔ عادی سرویس[2]: این نوع تهدید به صورتی است که حتی کاربران مجاز نیز از دسترسی به سرویس‌های سامانه منع می‌شوند (برکتین، ۱۱:۱۳۸۵).

۸- تغییر سطوح دسترسی[3]: در این نوع تهدید کاربر بدون کسب اجازه از مقام بالاتر در سامانه، حقوق و سطوح دسترسی خود را افزایش داده و سپس تهدید خود را عملی می‌کند (برکتین، ۱۲:۱۳۸۵).

جمع‌بندی مباحث نظری: با توجه به احصای تهدیدهای حوزهٔ این فناوری و همچنین اطلاعات طبقه‌بندی‌شده از طریق مطالعه و بررسی مباحث نظری در راستای تدوین الزامات مربوطه، مصاحبه با خبرگان نشان داد که علاوه بر این تهدید نقاط آسیب‌پذیر دیگری نیز به‌ویژه در زمینهٔ به‌کارگیری این فنآوری وجود دارد. جمع‌بندی کلیه آسیب‌پذیری‌های موجود به‌عنوان شاخص‌های تأثیرگذار در احصای الزامات این حوزه در جدول شماره ۱ ارائه شده است.

جدول شماره ۱: نقاط آسیب‌پذیر مؤلفه‌های مؤثر در به‌کارگیری RFID.

ابعاد	مؤلفه‌ها	نقاط آسیب‌پذیر
امنیت چرخه حیات اطلاعات	تولید اطلاعات	نبود طبقه‌بندی و علامت‌گذاری صحیح مدارک و تجهیزات.
		نبود طبقه‌بندی صحیح ضمایم مدارک و تجهیزات و ایجاد زمینه دسترسی غیرمجاز به آن‌ها.
	توزیع اطلاعات	نبود ردیابی و کنترل مداوم و برخط مدارک و تجهیزات در فرآیند توزیع.
		نبود نظارت بر مدارک و تجهیزات تکثیرشده و ایجاد زمینه دسترسی غیرمجاز.
	بهره‌برداری از اطلاعات	دسترسی غیرمجاز و نبود تطبیق صلاحیت افراد با سایر متغیرهای امنیتی اطلاعات.
		ثبات متغیرهای امنیتی اطلاعات (طبقه‌بندی و...) علی‌رغم تغییر در اهمیت اطلاعات.
	نگهداری اطلاعات	نبود نظارت دقیق بر نقل‌وانتقال مدارک و تجهیزات در اماکن نگهداری آن‌ها.
		تداخل حیطه‌های نگهداری مدارک و تجهیزات دارای شناسه با سایر مدارک و تجهیزات.
		نبود تغییر در متغیرهای امنیتی (طبقه‌بندی و...) متناسب با سایر تغییرات.
	امحاء اطلاعات	نبود اطلاع برخط از زمان امحای اطلاعات و انباشت اطلاعات فاقد نیاز.
		نبود ممیزی دقیق فرآیند کامل امحا.
نیروی انسانی کاربر فنآوری	مدیر سیستم	عدم توجه به صلاحیت‌های فنی و امنیتی مدیر سیستم.
		ایجاد زمینه گسترش تهدید به دلیل نبود ارتقای سطح دانش فنی و امنیتی
		امکان بروز تهدید علیه سامانه به دلیل نبود نظارت بر عملکرد مدیر سیستم.
		نبود برخورد نظام‌مند با اقدام‌های غیرمجاز و تخلفات در فرآیند مدیریت سامانه.
	بهره‌بردار	بی‌توجهی به صلاحیت و سطح دسترسی کاربران و ایجاد زمینه تهدید از این طریق.

1 - Evident of Information
2 - Inhibition of Normal Service
3 - Change Access Level

		فقدان آموزش حفاظتی و کاربری کاربران و گسترش آسیب‌های وارده از جانب آن.
		نبود نظارت و کنترل بر عملکرد فنی و امنیتی کاربران.
		فقدان فرآیندهای قانونی جهت برخورد با اقدام‌های غیرمجاز کاربران.
امنیت زیرساخت فناوری (اجزاء)	شناسه (Tag)	بومی نبودن شناسه و ایجاد زمینه تهدید در فرآیند تأمین.
		ایجاد زمینه تهدید فیزیکی و غیر فیزیکی علیه شناسه در فرآیند به‌کارگیری.
		بروز مشکلات فنی و امنیتی در عملکرد شناسه و ایجاد زمینه آسیب از جانب آن.
		دسترسی غیرمجاز به شناسه‌های معیوب یا فاقد کاربری و بروز تهدید از جانب آن.
	بازخوان (Reader)	بومی نبودن بازخوان و ایجاد زمینه تهدید در فرآیند تأمین.
		ایجاد زمینه تهدید فیزیکی و غیر فیزیکی علیه بازخوان در فرآیند به‌کارگیری.
		بروز مشکلات فنی و امنیتی در عملکرد بازخوان و ایجاد زمینه آسیب از جانب آن.
		دسترسی غیرمجاز به بازخوان‌های معیوب یا فاقد کاربری و بروز تهدید از جانب آن.
	نرم‌افزار کنترل‌کننده	امکان آلوده سازی نرم‌افزار، در فرآیند تأمین و زمینه‌سازی دسترسی غیرمجاز.
		نبود نظارت بر حیطه‌بندی و دسترسی به نرم‌افزار در فرآیند نصب و کاربری.
		نبود ارزیابی فنی و امنیتی نرم‌افزار و بی‌توجهی به رفع نقاط آسیب‌پذیر احصا شده.

روش تحقیق، جامعه آماری، تجزیه تحلیل و اثبات فرضیه ها

به‌کارگیری فنآوری RFID به همان صورتی که هست در مقاله مطالعه و به همین علت از روش توصیفی استفاده شده است. جامعهٔ آماری شامل ۵۰ نفر از کارشناسان حوزه‌های حفاظتی و امنیتی می‌باشند که با توجه به دسترسی به آن‌ها، جامعه نمونه‌ای انتخاب نشد.

علاوه بر انجام مصاحبه، از یک ابزار محقق ساخته ۳۵ سؤالی استفاده شده که در طیف لیکرت طراحی گردیده است. روایی آن از طریق روایی صوری بررسی و اعتبار آن از طریق آلفای کرونباخ محاسبه که ارزش آن در این تحقیق برابر ۹۴/. است.

برای تجزیه‌وتحلیل اطلاعات با بهره‌برداری از دو روش کمی شامل آمار توصیفی (جداول شاخص‌های آماری، فراوانی و نمودار ستونی) و نیز آمار استنباطی (آزمون خی دو) ونیز مصاحبه با خبرگان این حوزه استفاده شد.

فرضیهٔ ۱: الزامات چرخهٔ حیات اطلاعات به‌وسیلهٔ فنآوری RFID در راستای ارتقای امنیت اطلاعات طبقه‌بندی‌شده ودجا عبارتند از؛ امنیت تولید اطلاعات، امنیت توزیع اطلاعات، امنیت بهره‌برداری اطلاعات، امنیت نگهداری اطلاعات و امنیت امحای اطلاعات.

داده‌های به‌دست‌آمده در خصوص فرضیهٔ شماره ۱ نشان می‌دهد که میانگین، میانه و انحراف استاندارد توزیع به ترتیب ۴/۰۵، ۴ و ۰/۸۲ است. توزیع از کجی منفی برخوردار بوده و در نقطه اوج خود نسبت به توزیع نرمال دارای خوابیدگی جزئی است. کمینه و بیشینه نمرات نیز بین ۱ تا ۵ در نوسان است. توزیع مربوط به فراوانی نیز نشان می‌دهد که ۷۶/۵ درصد

پاسخ‌دهندگان در حد زیاد و خیلی زیاد نسبت به محتوای فرضیهٔ شماره ۱ نظر مساعدی دارند. همچنین آزمون خی دو فرضیه‌ی یک نشان می‌دهد ارزش خی‌دوی مشاهده‌شده (۳۸۶/۹۲) در درجه آزادی ۴ معنی‌دار است. درنتیجه استنباط می‌شود که فرضیهٔ شماره ۱ مورد تأیید است.

فرضیهٔ شماره ۲: الزامات نیروی انسانی کاربر فنآوری RFID در راستای ارتقای امنیت اطلاعات طبقه‌بندی‌شده ودجا عبارتند از: الزامات مدیر سامانه و بهره‌بردار.

داده‌های به‌دست‌آمده در خصوص فرضیهٔ شماره ۲ نشان می‌دهد که میانگین، میانه و انحراف استاندارد توزیع به ترتیب ۴/۱۵، ۴ و ۰/۸۲ است. توزیع از کجی منفی برخوردار بوده و در نقطه اوج خود نسبت به توزیع نرمال دارای برآمدگی جزئی است. کمینه و بیشینه نمرات نیز بین ۱ تا ۵ در نوسان است. توزیع مربوط به فراوانی نیز نشان می‌دهد که ۸۰ درصد پاسخ‌دهندگان در حد زیاد و خیلی زیاد نسبت به محتوای فرضیه‌ی دو نظر مساعدی دارند.

همچنین آزمون خی دو فرضیهٔ شماره ۲ نشان می‌دهد ارزش خی‌دوی مشاهده‌شده (۳۳۵/۲۴) در درجه آزادی ۴ معنی‌دار است. درنتیجه استنباط می‌شود فرضیهٔ شماره ۳ مورد تأیید است.

فرضیهٔ شماره ۳: الزامات امنیت زیرساخت فنآوری RFID در راستای ارتقای امنیت اطلاعات طبقه‌بندی‌شده ودجا عبارتند از: امنیت شناسه، امنیت بازخوان و امنیت نرم‌افزار کنترل‌کننده.

داده‌های به‌دست‌آمده در خصوص فرضیه سه نشان می‌دهد که میانگین، میانه و انحراف استاندارد توزیع به ترتیب ۴/۱۸، ۴ و ۰/۸ است. توزیع از کجی منفی برخوردار بوده و در نقطه اوج خود نسبت به توزیع نرمال دارای برآمدگی است. کمینه و بیشینه نمرات نیز بین ۱ تا ۵ در نوسان است. توزیع مربوط به فراوانی نیز نشان می‌دهد که ۸۲.۴ درصد پاسخ‌دهندگان در حد زیاد و خیلی زیاد نسبت به محتوای فرضیهٔ شماره ۳ نظر مساعدی دارند.

همچنین آزمون خی دو فرضیهٔ شماره ۳ نشان می‌دهد ارزش خی‌دوی مشاهده‌شده (۶۰۶/۲۹) در درجهٔ آزادی ۴ معنی‌دار است. درنتیجه استنباط می‌شود فرضیهٔ شماره ۳ مورد تأیید است.

نتیجه‌گیری و پیشنهاد

با توجه به اینکه هر سه فرضیهٔ فرعی مورد تأیید قرار گرفت و هر سه تشکیل‌دهندهٔ فرضیه اصلی بودند، بنابراین نتیجهٔ تجزیه‌وتحلیل اطلاعات پژوهشی، احصای الزامات، آزمون برگزارشده و جمع‌بندی پاسخ‌های اخذشده در خصوص فرضیه‌های مطرح‌شده درنهایت منتج به احصای الزامات ارتقای سطح امنیت اطلاعات طبقه‌بندی‌شده ودجا با استفاده از فنآوری RFID گردیدند. الزامات تدوین‌شده در این مقاله که در راستای تحقق اصل شانزدهم پدافند غیرعامل با چهارده الزام، شاخصه‌های پدافند غیرعامل با سیزده الزام و کارکردهای حفاظتی پدافند غیرعامل اعم از

حفاظت سایبری از کشور و حفاظت از تأسیسات و تجهیزات نادر با پنج الزام احصا گردیده‌اند. درمجموع شامل ۳۵ الزام در زمینهٔ امنیت چرخه حیات اطلاعات به‌وسیله این فناوری، نیروی انسانی کاربر آن و نیز امنیت زیرساخت این فناوری مبتنی بر ابعاد اصلی زیر می‌باشند که با اجرای آن می‌توان امنیت به‌کارگیری فنآوری RFID و به‌تبع آن مدارک و تجهیزات حامل شناسه RFID را ارتقا داد:

الف) الزامات امنیت چرخهٔ حیات اطلاعات به‌وسیله فنآوری RFID

این حوزه شامل یازده الزام است که در پنج مؤلفه ازجمله «امنیت تولید، امنیت توزیع، امنیت بهر برداری، امنیت نگه‌داری و امنیت فرآیند امحای اطلاعات» تدوین گردیده‌اند. «درج متغیرهای امنیتی اطلاعات (طبقه‌بندی، سطوح دسترسی و...) در سامانه و شناسه، پوشش حداکثری اجزا و ضمایم مدارک و تجهیزات، ردیابی و کنترل مداوم و برخط مدارک و تجهیزات، همچنین پوشش حداکثری اسناد و مدارک تکثیرشده به‌وسیله این فنآوری، کنترل و تطبیق دسترسی افراد، امکان تغییر در متغیرهای امنیتی اطلاعات به‌وسیله این فنآوری، امکان رصد مداوم مدارک و تجهیزات در اماکن نگهداری، جداسازی حیطه‌های مربوط به اماکن نگهداری مدارک و تجهیزات، انعکاس هرگونه تغییر در متغیرهای امنیتی به مراجع نگهداری، امکان اطلاع برخط از زمان امحای اطلاعات و همچنین امکان ممیزی فرآیند کامل امحاء اطلاعات با استفاده از سامانه RFID» ازجمله الزامات احصای شده در حوزهٔ امنیت چرخهٔ حیات اطلاعات می‌باشند.

ب) الزامات نیروی انسانی کاربر فنآوری RFID (امنیت کاربری)

این حوزه شامل ۹ الزام است که در دو مؤلفه ازجمله «مدیر سامانه و بهره‌بردار (کاربر)» تدوین گردیده‌اند. در بخش مدیران سامانه «توجه به صلاحیت‌های فنی و امنیتی، آموزش و ارتقای سطح دانش فنی و امنیتی، ارزیابی فنی و امنیتی عملکرد و همچنین تدوین فرآیندهای قانونی برای برخورد با اقدام‌های غیرمجاز» و در بخش کاربران «تعیین صلاحیت و سطح دسترسی، توجه به آموزش حفاظتی و کاربری، نظارت و کنترل بر عملکرد فنی و امنیتی و همچنین تدوین فرآیندهای قانونی جهت برخورد با اقدام‌های غیرمجاز کاربران» ازجمله الزامات احصاء شده در حوزه نیروی انسانی کاربر سامانه RFID می‌باشند.

ج) الزامات امنیت زیرساخت فنآوری RFID (امنیت اجزاء سامانه)

این حوزه شامل پانزده الزام است که در سه مؤلفه ازجمله «امنیت شناسه، امنیت بازخوان و امنیت نرم‌افزار کنترل‌کننده» تدوین گردیده‌اند. «توجه به امنیت زنجیره تأمین شناسه، رفع

نقاط آسیب‌پذیر فیزیکی و غیرفیزیکی، بررسی مداوم عملکرد فنی و امنیتی و تأمین امنیت شناسه‌های معیوب یا فاقد کاربری، توجه به امنیت زنجیره تأمین بازخوان، رفع نقاط آسیب‌پذیر فیزیکی و غیرفیزیکی، بررسی مداوم عملکرد فنی و امنیتی و تأمین امنیت بازخوان‌های معیوب یا فاقد کاربری، توجه به امنیت نرم‌افزار در فرآیند تأمین و پشتیبانی، نظارت بر حیطه‌بندی و دسترسی به نرم‌افزار و همچنین ارزیابی فنی و امنیتی نرم‌افزار و رفع نقاط آسیب‌پذیر احصا شده» ازجمله الزامات احصا شده در حوزهٔ امنیت اجزای سامانه RFID می‌باشند.

منابع

۱. اسکندری، حمید، (۱۳۹۱)، ***دانستنی‌های پدافند غیرعامل***، تهران، بوستان حمید.

۲. اکبرپور، مجید، (۱۳۹۱)، ***گزارش امنیت در فنآوری و ارتباطات***، دانشکده علوم و فنون فارابی.

۳. امینی لاری، منصور، کارشناس، الهام، (۱۳۸۶)، ***به‌کارگیری فناوری RFID در تجارت الکترونیکی بین بنگاهی***، دومین کنفرانس بین‌المللی RFID.

۴. باقریان، حمید، (۱۳۸۵)، ***حفاظت اسناد***، تهران، مؤسسه تحقیقاتی پژوهشی حفیظ.

۵. برکتین، بهرنگ، (۱۳۸۵)، ***معرفی مدل نه وجهی FAST MEDIC برای تهدیدهای امنیتی در RFID***، اولین کنفرانس بین‌المللیRFID.

۶. ترحمی، مهران، صالحی، سیما، (آذر ۸۸)، ***آسیب‌شناسی سیستم‌های اطلاعات جغرافیایی با رویکرد پدافند غیرعامل ICT***، همایش سراسری سامانه اطلاعات مکانی (GIS)، انجمن علمی فنآوری اطلاعات و ارتباطات ودجا، سازمان جغرافیایی.

۷. جان‌نثاری لادانی، مجید، صفری، حسین و عظیمی، علی، (۱۳۸۶)، ***ریسک‌های امنیتی سیستم‌های RFID***، دومین کنفرانس بین‌المللی RFID.

۸. جلالی، غلامرضا، (۱۳۹۱)، ***چهارگفتار در باب پدافند غیرعامل***، تهران: انتشارات محدث.

۹. جلالی، غلامرضا، (۱۳۹۰)، ***کلیات پدافند غیرعامل***، دانشگاه فارابی.

۱۰. جلالیان، خسرو، مردادی، فریال، علیدوست، هنگامه، ایزی، زهرا، (۱۳۹۰)، ***سیستم شناسایی از طریق امواج رادیویی***، مرکز تحقیقات صنعتی ایران.

۱۱. جواهری، حمیدرضا، (۱۳۸۷)، ***کاربرد فنآوری RFID در هوشمند سازی و ارتقاء امنیت اسناد و مدارک***، تهران، دانشکده امام باقر (ع).

۱۲. دولت‌آبادی، حسن، بخشی زاده، سعید، (۱۳۸۶)، ***شناخت RFID و تهدیدهای پیش رو***، سازمان حفاظت اطلاعات ودجا.

۱۳. روهینا، محمد، حسام زاده، شهرام، کراری، حبیب، نجاری، حسین، (۱۳۸۵)، ***نرم‌افزارهای مشکل‌ساز RFID***، اولین کنفرانس بین‌المللی RFID.

۱۴. ساحفا ودجا، (۱۳۹۱)، ***آشنایی با حفاظت اطلاعات***، تهران، موسسه ایز ایران.

۱۵. ستاد کل نیروهای مسلح، (۱۳۷۵)،***آئین‌نامه حفاظت از اسناد و مدارک طبقه‌بندی‌شده***.اسناد و مدارک داخلی.

۱۶. ستاد کل ن.م، (۱۳۹۱)، ***پیش‌نویس الگوی سامانه شناسایی مبتنی بر فنآوری RFID.***

۱۷. شرکت ایزایران، (۱۳۸۹)، ***سند راه‌حل فنی مدیریت و مانیتورینگ کالا***.

۱۸. سلیمانی، صادق، (۱۳۸۵)، ***چالش‌های RFID بر شبکه، اولین کنفرانس بین‌المللی RFID.***

۱۹. سلیمانی، صادق، کاغذگران، پریسا، (۱۳۹۰)، ***تشخیص دست‌کاری در داده‌های برچسب RFID با استفاده از نشانه گذاری شکننده***، هشتمین کنفرانس بین‌المللی انجمن رمز ایران.
۲۰. علوی فر، سیدناصر، (۱۳۸۵)، ***راهکارهای تأمین و توسعه امنیت***، تهران، جهانگیر.
۲۱. عموزاد خلیلی، حسین، آیانی، سپیده، حق‌پرست، آیدین، (۱۳۸۶)، ***تبیین و تحلیل قابلیت‌ها و محدودیت‌های پیشبرد فناوری RFID در توسعه پایدار***، دومین کنفرانس بین‌المللی RFID.
۲۲. مقدسی، سعید، سبحان منش، فریبرز، مقدسی، حمید، (۱۳۸۸)، ***اصول سیستم‌های شناسایی از طریق فرکانس‌های رادیوئی و کاربردهای آن***، چاپ اول تهران، رستار.
23. Wyld, D.C. (2006), "**RFID 101: the next big thing for management**" Management Research News 29 (4), pp. 154–173
24. Potter, B. (2005), "**RFID: misunderstood or untrustworthy?**" Network Security, April, pp. 17-18.