مسائل امنیت اطلاعات RFID (سیستم بازشناسی با امواج رادیویی)

چکیده :

بعد از ارایه یک تاریخچه کوتاه از RFID، نویسنده این مقاله، به بحث در مورد مسائل عمومی و امنیتی مربوط به RFID و راه حل های احتمالی آن ها می پردازد. امنیت اطلاعات به صورت یک بخش اساسی و جدایی ناپذیر از امنیت کل ارزیابی می شود. به علاوه، راه حل های مختلف امنیت اطلاعات و فناوری ها برای حل مسائل امنیت خاص ارایه می شود. از طیف وسیعی از امکانات کاربرد، نویسنده، حفاظت اسناد و امنیت اداری را انتخاب کرده است. مستند سازی مبتنی بر کاغذ را نمی توان از زندگی روزمره جدا گرد. اگرچه پیشرفت زیادی در زمینه ابزار های معتبر و چک های تضمین شده وجود داشته است، بسیاری از عناصر امنیتی در زندگی روزمره امروزی هنوز دیده نمی شود. امکانات کاربردی کاغذ" هوشمند" و علامت دیجیتال را می توان در این جا در نظر گرفت. در زمان بررسی مسئله توسعه و پیشرفت آینده، نویسنده برخی از جایگزین های احتمالی پیش بینی شده توسط کارشناسان صنعت را برای سال های آینده ارایه می کند.

1- مقدمه کلی در خصوص RFID

RFID (سیستم باز شناسی با امواج رادیویی) یک فناوری ای است که از کوپلینگ یا جفت شدگی الکترواستاتیک یا الکترو مغناطیسی را در بخش فرکانس رادیویی (RF) طیف الکترومغناطیسی برای شناسایی منحصر به فرد یک شی، حیوان یا انسان بهره می برد. RFID در صنعت به عنوان جایگزین بارکد در حال افزایش است. مزیت RFID این است که نیازی به تماس مستقیم یا اسکن خط دید ندارد. یک سیستم RFID متشکل از سه مولفه است: یک آنتن و گیرنده فرستنده(اغلب به یک خواننده تلقیق می شود) و یک ترنسپوندر(شناسه). آنتن از امواج فرکانس رادیویی برای انتقال یک سیگنال استفاده می کند که این سیگنال موجب فعال سازی ترنسپوندر می شود. وقتی که شناسه فعال سازی شد، شناسه داده ها را به آنتن بازمی گرداند(1).

الف: تاریخچه مختصر در خصوص RFID

نخستین فناوری بازشناسی با امواج رادیویی در طی جنگ جهانی دوم توسعه یافت. رابرت الکساندر واتسون، رادر را کشف و کامل کرد که این رادار تنها برای کشف و تشخیص استفاده می شد. با این حال این رادار قادر به شناسایی نبود. در 1929، دانشمندان انگلیسی، به طور تصادفی کشف کردند که وقتی خلبان یک جنش نوسانی در هواپیما ایجاد می کند، شکل امواج رادیویی بازتاب شده تغییر می کند و این امکان تفکیک بین هواپیمای دشمن و هواپیمای خودی را در صفحه رادار می دهد. این را می توان به صورت نخستین سیستم RFID غیر فعال در نظر گرفت که در نهایت منجر به توسعه اولین سیستم تشخیص هواپیمای فعال یعنی IFF شد. اوج شکوفایی فناوری RFID در 1970 میلادی بعد از معرفی آن در 1960 صورت گرفت. مطالعات ار. اف هارینگتون بر روی میدان های الکترومغناطیسی، مبنایی برای توسعه RFID آینده بود. اولین کاربرد تجاری آن در اوایل 1960 میلادی شروع شد. سنسورماتریک یک شرکت پشرو در توسعه راه حل های RFID بود. سیستم ضد سرقت EAS هنوز یک فناوری پر کاربرد می باشد. پیشرفت های عمده هم در اروپا و هم در آمریکا در دهه 1970 میلادی برای معرفی RFID در پایش حیوانات، وسایل نقلیه و فرایند های تولید صورت گرفت. بعدها پایش و ردیابی دام ها و چارپایان توسط کشاورزان و دامپروران به طور گسترده ای رواج یافت. موسسه تحقیقات آلاموس لس یک سیستمی را برای ردیابی دستگاه های هسته ای در طی این سال ها توسعه یافت. در 1980 میلادی، بعد از مرحله تحقیق و توسعه ، پیاده سازی راه حل های جدید و کاربرد آن ها در محصولات مختلف صورت گرفت. در ایالات متحده، این سیستم در ابتدا برای ردیابی و پایش فرایند های تحویل، به منظور اطمینان از دسترسی شخصی و شناسایی حیوانات استفاده می شد. در 1990 میلادی، دامنه کاربرد های RFID گسترده تر شد: این سیستم در عوارضی های بزرگ راه ها و نیز در ایموبلایزر ها یا بلیط های فصلی(اسکی بازی) معرفی شد. اولین دیود شاتکی مایکروویو تلفیق شده بر روی مدار های CMOS، امکان ایجاد شناسه های RFID مایکرویو با یک تک IC را داد به طوری که دامنه خواندن بزرگ تر شده و سرعت انتقال داده ها سریع تر گردید. UHF RFID در 1999 زمانی که مرکز شناسایی اتوماتیک تاسیس شد، تحول عظیمی را تجربه کرد. این شرکت یک شناسه RFID کم هزینه را توسعه داد که حاوی یک ریزتراشه است. شناسه تنها برای ذخیره شماره سریال استفاده می شود که نیازمند حافظه کوچک تری

است و از همین روی ارزان نیز می باشد. شماره سریال در دیتابیس اینترنتی برای دریافت اطلاعات بیشتر در مورد محصول قابل جست وجو است. قبل از این، RFID TAG به عنوان یک دیتابیس سیار بوده است. امروزه شرکت های تجاری بزرگ و چند ملیتی در حال برنامه ریزی برای پیاده سازی کامل RFID می باشند. علاوه بر وزارت دفاع امریکا، شرکت های تولید تایر و دارویی مختلف به فناوری علاقه مند بوده اند. در واقع، استفاده گسترده از RFID را می توان در حال حاضر بعد از تایید استاندارد های نسل دوم توسط EPCglobal انتظار داشت(2).

ب: کاربرد های احتمالی RFID

- لجستیک، انبار های تجاری؛
- برنامه های کتابخانه ای و بایگانی.
- ردیابی دارایی ها، موجودی دارایی؛
- بهینه سازی تولید؛
- مدیریت زنجیره تامین؛
- تجارت خرده فروشی؛
- سیستم های عوارض؛
- سیستم های کنترل امنیتی و دسترسی.
- دام ها و چارپایان [3]

پ: شناسه های RFID طبقه بندی شده

جدول 1: شناسه های RFID به صورت کلاس 0 تا 5 بسته به کارکرد خود طبقه بندی می شوند

کلاس 0	UHF صرفا خواندنی، تگ غیر فعال پیش برنامه ریزی شده
کلاس1	UHF یا HF، خواندن توزیعی و نوشتن تجمعی WORM
کلاس2	تگ های نوشتن-خواندن غیر فعال که می توان آن ها را در هر نقطه در زنجیره تامین نوشت
کلاس3	خواندن-نوشتن با سنسور های آنبورد که قادر به ثبت پارامتر هایی نظیر دما، فشار و حرکت می باشند، می تواند به صورت نیمه منفعل یا فعال باشد

کلاس4	شناسه های فعال خواندن-نوشتن با فرستنده های تلفیقی: قادر به برقراری ارتباط با سایر شناسه ها و خواننده ها می باشد
کلاس5	مشابه با شناسه های کلاس 4 است، با این حال دارای کارکرد بیشتری است. می تواند توان را برای سایر شناسه ها ارایه کند و با دستگاه هایی به غیر از خواننده ها ارتباط برقرار می کند.

ت: سوالات و نگرانی ها در خصوص RFID

استفاده از RFID برای اطلاعات قابل شناسایی شخصی برای سالیان متمادی موضوع مطالعات و بحث های زیادی بوده است. این خود موجب بروز مسائلی در مورد حفاظت از داده های شخصی می شود. نگاه افراد به تهدید طوری است که شناسه های RFID می تواند بدون مجبور بودن برای مواجهه با مالک خوانده شود زیرا شناساگر منحصر به فرد مهر ها می تواند مربوط به داده های شخصی مالک باشد. به علاوه، شناسه های RFID می توانند بر روی هر گونه کالا بدون دانش مشتری قرار داده شود.به علاوه، شناسه ها می توانند توسط خواننده ها به صورت از راه دورخوانده شوند از این روی یک فرد ممکن است از خوانده شدن شناسه آگاه نباشد. برای مثال، یک مشتری نمی تواند شناساگر ها را در یک فروشگاه غیر فعال کند.وقتی که پرداخت توسط کارت بانکی انجام شد، محصول خریداری شده را می توان به مشتری ارتباط داد. در نتیجه، مشتری را می توان بر اساس نام شناسایی کرد. از این روی، امکان رد یابی نه تنها محصول، بلکه رد یابی مشتری از راه دور وجود دارد. گیت های غیر فعال سازی مختلف قبلا مورد استفاده قرار گرفته اند با این حال کارایی آن ها هنوز مورد سوال است.البته، سیگنال های رادویی را می توان با روش های رمزنگاری مختلف رمزنگاری کرد. علاوه بر حفاظت از حریم خصوصی، مسئله مهم دیگر این است که آیا RFID برای سلامت یا محیط مضر است یا خیر.میدان های الکترومغناطیسی مربوط به RFID به طور کلی ضعیف هستند و جمعیت در معرض تابش با نرخ کم تر از آستانه های استاندارد جاری قرار می گیرند. با این وجود، تعداد دستگاه های بی سیم تا کنون افزایش یافته است(5).

2-RFID و امنیت

اخیرا، پیاده سازی سیستم های RFID در کاربرد های با امنیت بالا مورد توجه قرار گرفته است. در این رابطه می توان به شناسایی بیمار یا سیستم پرداخت کارت اعتباری پی پس رایج را در نظر گرفت. این راه

حل ها مستلزم یکپارچه سازی مکمل های امنیتی خاص با سیستم های موجود است که قادر به پیش گیری از دسترسی یا ورود غیر مجاز هستند. این سیستم های احراز هویت پیشرفته، حقیقت داشتن رمز را آشکار می کنند. هدف استفاده از الگوریتم مناسب، پیش گیری از به خطر افتادن یا فاش شدن کلید خصوصی است. سیستم های RFID با امنیت بالای امروزه، قادر به پیشگیری از حملات زیر هستند:

- دسترسی غیر مجاز به رسانه ها با هدف کپی برداری یا تغییر داده های ذخیره شده
- قرار دادن رسانه های با مبدا ناشناخته در منطقه با غلبه بر الگوریتم های احراز هوایت
- قطع ترافیک رادیویی یا ایجاد یک تصویر کاذب از پخش رسانه های معتبر(بازپخش و جعل)(2)

الف: احراز هویت متقارن متقابل

احراز هویت متقارن متقابل بر اساس روش سه مرحله ای بین خواننده و ترنسپوندر بر طبق استاندارد ISO 9798.2 می باشد که همزمان دانش دو طرف را از کلید رمزنگاری رمز کنترل می کند(2).

ب:احرازاصالت کلید استخراج شده

هر ترنسپوندر مجهز به یک کلید خصوصی به منظور بهبود ایمنی است. برای دست یابی به این هدف ابتدا شماره سریال ترنسپوندر بایستی استخراج شود. کلید رمز با کمک یک شاه کلید و الگوریتم رمزنگاری ایجاد می شود. در نتیجه، هر ترنسپوندر، ID خاص و یک شماره سریالی را دریافت می کند که متصل به شاه کلید بر روی کانال پایین لینک است. خواننده به عنوان اولین مرحله احراز اصالت و احراز هویت، شناسه ترنسپوندر را بازیابی می کند. با کمک شاه کلید، ماژول رمزگاری خاص خواننده، ایجاد یک کلید خصوصی خواننده را می کند(2).

پ: اتصال رمزنگاری شده

راه حل توصیف شده در فصول قبلی در حال حاضر با یک مهاجم بالقوه کامل یم شود. در این رابطه، دو نوع مهاجم وجود دارد. نوع اول سعی می کند تا در پس زمینه باقی بماند و اطلاعات ارزشمند را به شکلی غیر فعال از طریق حایل شدن بازیابی کند. با این حال، دومین نوع مشارکت فعالی در مبادله داده ها دارد و محتوی آن را برای استفاده خود تغییر می دهد. راه حل های رمز نگاری را می توان در برابر هر دو نوع مهاجم استفاده

کرد. ارزش داده ها رمزنگاری شده و در نتیجه، مهاجم قادر به استخراج اطلاعات و نتیجه گیری در مورد محتوی اصلی آن نخواهد بود. رمز لینک داده ها براساس یک اصل مشابه عمل می کند. در رابطه با رمزگذاری دنباله ای، هر کاراکتر به طور جداگانه رمز گذاری می شود در حالی که در رمز گذاری کد گذاری بلوکی با بلوک های کاراکتر انجام می شود. بزرگ ترین مسئله و مشکل مربوط به سیستم های RFID با ترافیک داده های رمز گذاری شده، توزیع کلید متقارن قبل از استفاده از آن است(2).

انکودر های استریم،مجموعه ای از الگوریتم های رمزنگاری هستند که کاراکتر های متن باز را به طور متوالی و دنباله ای ولی با کارکرد های متفاوت رمز گذاری می کنند. در ابتدا، یک کلید تصادفی ایجاد خواهد شد که کلید را بین طرفین مبادله اطلاعات به اشتراک می گذارد. سپس این کلیئ دارای یک اتصال XOR با کاراکتر های متن باز خواهد بود. کلید تصادفی بایستی حداقل دارای طول یکسان و برابر با متن باز باشد در غیر این صورت حملات آماری الگوهای تکراری را می توان انتظار داشت. به علاوه، هر کلید تنها یک بار استفاده می شود که نیازمند سطح بالایی از ایمنی در توزیع کلید است. رمز گذاری استریم به این شکل، برای سیستم های RFID کاملا نامناسب است. به منظور غلبه بر برخی از پیچیدگی های ناشی از تولید و توزیع کلید، مولد های اعداد تصادفی واقعی با مولد های شبه تصادفی همراه با کلید های شبه تصادفی(2) جایگزین شده اند.

ت: سایر توصیه های امنیتی

در رابطه با کنترل دسترسی هش-محور، با در نظر گرفتن مدیریت منابع ارزان شناسنه های هوشمند ارزان، یک روش امنیتی ساده بر اساس توابع هش یک سویه می باشد که در زیر ارایه شده است. معمولا، طرح با سخت افزار پیاده سازی می شود. شناسه هایی که در حالت قفل شده یا باز کار می کنند یک بخش کوچک از حافظه خود را برای ذخیره شناسه متا جدا می کنند. به منظور قفل کردن یک شناسه، مالک آن، نسخه هش شده کلید تصادفی را به صورت شناسه متای تگ در ترنسپوندر ذخیره می کند. این کار را می توان توسط RF و یا به روش فیزیکی مستقیم انجام داد. به منظور باز کردن کلید، هاست، شناسه متا را بازیابی کرده و کلید را در دیتابیس پیدا می کند و سپس آن را به ترنسپوندر باز می گرداند. شناسه کلید را هش می کند و آن را با شناسه متای خود مقایسه می کند. به محض این که این دو هش با یک دیگر ارتباط

برقرار کنند، کلید خودش را باز می کند و کارکرد کاملی را برای خواننده های مجاور فراهم می کند. به منظور پیش گیری از هر گونه سو استفاده از شناسه های باز، شناسه ها بایستی تنها برای مدت زمان جریان اطلاعات باز بمانند. این روش محافظت زیادی در برابر دسترسی غیر مجاز با استفاده از مسئله سخت بودن معکوس کردن هش یک سویه فراهم می کند. با این حال، این مانع از جعل نمی شود بلکه آن ها را تنها تشخیص می دهد. به علاوه، دستگاه خواننده می تواند محتوی شناسه ها را با کمک بک اند کنترل کند(2).

در رابطه با مورد کنترل دسترسی تصادفی، راه حل از توابع هش یک سویه استفاده می کند که برای تعداد کمی از شناسهها کارامد است و مانع از درخواست های غیر مجاز می گردد در حالی که شناسه ها قادر به پاسخ به درخواست خوانندگان مجاز هستند. علاوه بر ترنسپوندر های فوق الذکر که قادر به محاسبه توابع هش یک سویه می باشند، این راه حل قادر به تولید اعداد تصادفی است. با درخواست دستگاه خواننده، ترنسپوندر در ابتدا یک عدد تصادفی تولید می کند و سپس پیوستگی شناسه و اعداد تصادفی را از هش باز یابی می کند(2).

در رابطه با مذاکره کلید غیر متقارن، خوانندگان قادر به کسب اطلاعات بیشتری از عدم تقارن بین کانال های پایین لینک و بالا لینک در طی انتقال داده های حساس به دستکاری می باشند(2).

روش Chaffing and Winnowing موجب اختلال در تجهیزات رهگیری با پر کردن ارتباط با پیام های بلا استفاده یا پیام های بیهوده می شود که به طور پیوسته توسط ترنسپوندر ها با کمک یک MAC ساده در زمان ارسال داده های مفید فیلتر می شود(2). واحد های تشخیص را نیز می توان به سیستم RFID برای تشخیص خواندن غیر مجاز افزود. در رابطه با شناسه های صوتی، واحد های وفق را می توان به طور موفق در برابر حملات DoS مورد استفاده قرار داد زیرا آن ها را می توان برای تشخیص ترنسپوندر های خارج از حالت مورد استفاده قرار داد(2).

3- کاربرد RFID با توجه به امنیت سند

مفاهیم امنیت و ایمنی اشاره به امنیت اطلاعات/ امنیت داده های چاپ شده/ فتوکپی شده یا دیجیتال و نیز امنیت محصولات بسته بندی شده و برند در برابر دسترسی غیر مجاز یا دستکاری، حذف جزیی یا کامل،

آسیب یا تخریب دارند. این هم چنین به معنی حفاظت کامل از محرمانگی و صحت داده ها یا محصولات می باشد.

الف: سیستم حفاظت و امنیت داده ها

بسته به روش و درجه قابلیت شناسایی، راه حل های امنیتی دارای گروه های زیر می باشند:

- راه حل های امنیتی آشکار
- راه حل های امنیتی پنهان
- کاراکتر ها و نماد هایی که می توانند با ابزار های ماشینی، کاراکتر ها، خط، رنگ یا سایر دنباله های کد بازسازی شوند که با استفاده از تابش اشعه(لیزر،فرابفنش، مادون قرمز، رادیویی، اشعه ایکس و اشعه الکترونی) و یا معرف های شیمیایی قابل تشخیص هستند(6).

ب:راه حل های RFID برای مدیریت سند

شناسایی سند با استیکر های RFID

- RFID بر روی سند در شکل یک استیکر شناسایی استفاده می شود
- فناوری بدون برخورد، امکان شناسایی صدها سند در ثانیه را می دهد از این روی برای بایگانی ایده ال است
- مدیریت اسناد با سطح ایمنی بالا: استیکر قادر به ثبت این است که چه کسی، چه زمانی و چه مدت به سند دسترسی دارد(7)

مرکب های الکترونیکی(E-Inks)، نظیر موادی حاوی ذرات سفید با بار مثبت و محلول در مایع و ریزکپسوله های سیاه با بار منفی می باشند که بسته به قطبی بودن میدان مغناطیسی یا الکتریکی سفید یا سیاه می شود و توزیع صفحه ای آن ها حاوی اطلاعات بصری دو بعدی است(6).محلول های مرکب RFID مایع توسط مواد ارتباطات شناسه متقابل توسعه یافته و قادر به شناسایی مواد و محصولات افزوده شده با انتشار سیگنال های رادیویی می باشند. با افزودن این مایع به پرینتر و مرکب دستگاه فتوکپی، یک محصول چاپ با امنیت بالا و ضد سرقت را می توان تولید کرد(6). کاغذ هوشمند، که نوع رسانه آینده است را می توان با استفاده از

پلیمر های نیمه هادی، ریزتراشه ها، دستگاه های فرکانس رادیویی و عناصر الکترونیکی ترکیبی چاپ شده و قرار داده شده بر روی سطح کاغذ برنامه نویسی کرد(6). علامت دیجیتال(واترمارک دیجیتال) نخستین بار در بازار محصولات چاپی و فتوکپی شده در 1992 ظهور یافت. این می تواند برای مثال متشکل از ترکیبی از اعداد و کد باشد که تنها با یک دستگاه و یک امضای دیجیتال بازسازی می شود. علامت مرئی و نامرئی را می توان بر روی سطح محیط قرار داد و یا این که آن را در ماده محیط بسته به اهداف حفاظتی قرار داد(6).

4- پیش بینی ها، بازیگران و فرصت های RFID 2016-2026

بر طبق گزارش IDTechEx، در 2015، کل بازار RFID به ارزش 10.1 میلیارد دلار خواهد بود که 9.5 میلیارد در 2014 و 8.8 میلیارد دلار در 2013 است. این شامل شناسه ها، خواننده ها و نرم افزار ها و خدمات برای کارت های RFID، برچسب ها، فوب ها و همه ضرایب فرم دیگر برای هر دو RFID فعال یا غیر فعال می باشند.IDTechEx پیش بینی می کند که این رقم در 2020 به 13.2 میلیارد دلار افزایش یابد (8).

با استفاده از اطلاعات جدید و منحصر به فرد که در مقیاس جهانی توسط متخصصان فنی IDTechEx بررسی شده است، ما به تحلیل بازار RFID به شیوه های مختلف می پردازیم. تحلیل کامل توسط هر بازار به طور دقیق ارایه می شود از جمله داده های تاریخی عمقی با نوع کاربرد از 2005 به صورت سال به سال تا سال 2021 و با چشم اندازی به سال 2026.برای RFID غیر فعال، پیش بینی ها به طور جداگانه برای زمینه های کاربردی زیر ارایه می شوند. برای هر کدام، تعداد شناسه ها، قیمت فروش متوسط و ارزش کل شناسه ارایه می شود(2).

به علاوه، پیش بینی های ده ساله برای RFID و RTLS فعال و غیر فعال به کمک باطری در کاربرد های زیر ارایه شده است:

- داروسازی/مراقبت های درمانی
- زنجیره تامین خرده فروشی سرد
- کالاهای مصرف کننده

- پست
- قطعات و ابزار های تولیدی
- بایگانی(نمونه ها)
- نظامی
- مورد/پالت CPG خرده فروشی
- برچسب های لبه قفسه
- لوازم حمل و نقل، رول کیج،ULD،کیف
- وسایل نقلیه(به جز سایر بخش ها)
- ریموت ماشین ، سایر کاربرد های شناسه ای(8)

به علاوه، این گزارش واحد ها و ارزش کلی را برای RfID خوان ها به صورت زیر ارایه می کند

- پرتال ثابت UHF
- UHF توکار و دستی
- HF و LF دستی، ثابت، توکار
- ماشین LF
- موبایل NFC(8)

جدول 2: بخش های داده های بازاری UHF غیر فعال- پیش بینی ده ساله(8)

پیش بینی ده ساله بخش های داده های بازاری UHF غیر فعال	پیش بینی ده ساله بخش های داده های بازاری HF RFID غیر فعال	پیش بینی ده ساله بخش های داده های بازاری LF غیر فعال
خرده فروشی- لباس و کفش	کارت های بدون تماس هوشمند/فوب ها	چارپایان
خرده فروشی- سایر	بلیط های هوشمند	کنترل دسترسی
لجستیک، حمل و نقل، رول کیج	کتب	خودرو،ایموبلایزر

مدیریت دارایی، موجودی	پزشکی	پزشکی
پزشکی ومراقبت درمانی	دارایی و ابزار	افراد
چمدان و محموله	پاسپورت	سایر
کنترل دسترسی، صدور بلبط	افراد	
تعبیه شده	برنامه های NFC	
افراد	سایر	
سایر		

سپاسگزاری

تحلیل فعلی موضوع پوشش داده شده می تواند به توسعه سیستم های ثبت و شناسایی با امواج حال و آینده کمک کند. تضمین کیفیت و کاهش هزینه در فناوری اطلاعات نه تنها توسط دولت پشتیبانی می شود بلکه نقش رو به رشدی در هر دو بخش های خصوصی و سازمانی و نیز در بخش دولتی دارد. در نتیجه، شناسایی با امواج رادیویی و ملاحظات امنیتی مربوطه به طور روز افزونی پیشاپیش هر گونه پیشرفت و توسعه در سال های آینده خواهد بود. هدف اصلی توسعه این روش های شناسایی است که از منافع کاربران حفاظت کرده و مطابق با قوانین و قرار داد های حفاظت از داده های شخصی باشد. همان طور که مثال مربوط به امنیت اسناد فوق نشان داد، این راه حل ها کاربرد زیادی دارند و قادر به رفع نیاز های امنیتی امروزه با حداقل تلاش نوآورانه می باشند. تراشه های ارتباط رادیویی با فرکانس بالا که می توان آن را روی هر چیز و یا هر جا قرار داده و چاپ کرد در زمینه های مختلف از جمله لجستیک، تجارت، بهداشت درمان، امنیت مرزی، آموزش و اجرای قانون معرفی شده اند و به طور گسترده تری در آینده مورد استفاده قرار گرفته و تولید حجم زیادی از داده های پردازش شده خواهند کرد.