Survey of Security Solutions for Malware Detection in Identification Systems with Radio Frequency (RFID)

بررسی راهکارهای امنیتی جهت تشخیص بدافزارها در سامانه های بازشناسی با امواج رادیویی (RFID)

Kolsoum Saadian, Leila Ajam

Abstract — *Radio frequency identification (RFID) is a remote identification technique* ***that causes a change in Mode of using a specific object to identify in industry****. However, should* ***be considered*** *arrangements for protection against malware* ***threats*** *and users' information privacy and undetectablity of RFID.* ***Malwares are malicious software*** *in which* ***their main*** *purpose* ***is destruction of computer systems****.* ***Although the important information is stored in backend database****, they are threatened by SQL injection* ***and virus attacks*** *while* ***using RFID electronic tags****. At first the paper introduces RFID technology, and then be subjected to analysis in order to the effective diagnostic method of automatic SQL injection* ***prevent*** *the system away from contamination* ***and also Framework*** *to protect privacy of tag information* ***and*** *RFID system protection against* ***malwares****, Hence by using this framework****, RFID system be protected from malicious*** *software and tag's privacy protection will be insured.*[1].

Keywords — RFID, tag, reader, malwares, Security.

۱. چکیده

شناسایی فرکانس رادیویی (RFID) یک تکنیک شناسایی از راه دور است که باعث تحول در نحوه استفاده از یک شی خاص جهت شناسایی در صنعت شده است. با این حال با تمه‌یدات جهت محافظت در برابر تهدیدات بدافزارها و حفظ حریم خصوصی اطلاعات کاربران و غیرقابل‌ردیابی بودن RFID در نظر گرفته شود. بدافزارها نرم افزارهای مخربی هستند که هدف اصلی آنها تخریب سیستم‌های کامپیوتری می‌باشد. هر چند اطلاعات مهم در بخش مدیریت پایگاه داده ذخیره می شود ولی هنوز این بخش‌ها از طریق تذریق SQL و حملات ویروس در زمان استفاده از تگ‌های الکترونیکی RFID تهدید می‌شوند. در این مقاله ابتدا تکنولوژی RFID معرفی می‌شود، سپس روش تشخیص مؤثر خودکار تذریق SQL جهت جلوگیری از آلوده کردن سیستم و همچنین چارچوبی جهت حفظ حریم خصوصی اطلاعات تگ‌ها و حفاظت سیستم RFID از بدافزارها مورد بررسی و تحلیل قرار می‌گیرد، که با استفاده از این چارچوب، سیستم RFID از نرم افزارهای مخرب محافظت می‌شود و حفظ حریم خصوصی تگ نیز تضمین خواهد شد.

کلمات کلیدی

RFID ، تگ ، بازخوان ، بدافزارها، و امنیت

۲. مقدمه

RFID فناوری تایید شده از سال ۱۹۷۰ تاکنون است که بطور گسترده بصورت تجاری در صنعت مورد استفاده قرار گرفته است [۳]. این فناوری یک تکنولوژی بی سیم است که می‌تواند یک شی از راه دور را بدون تماس با استفاده از تگ شناسایی کند. تگ یک نهاد بسیار کوچک است که انرژی خود را از ورودی سیگنال رادیویی RF بدست می‌آورد. اندازه کوچک و ویژگی‌های بی‌قاعده آن، آن را برای کاربردهایی در زنجیره تأمین خرده فروشی، جایگزینی بارکد، شناسایی بیمار در مراقبت های بهداشتی و صنعت تولید و غیره مفید می سازد. با این وجود برنامه های سیستم RFID از حملات بدافزارها که شامل استثمارگرها، کرم ها و ویروس هستند مصون نیستند [۱]. بدافزارها از طریق تگ های RFID به سیستم های RFID انتقال یافته و سپس اجرا می‌شوند. ملاری R.Rieback و سایر همکاران

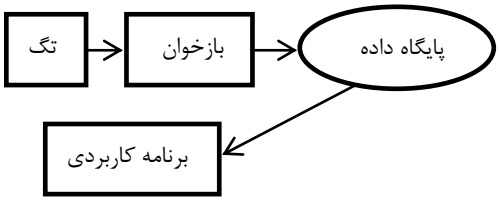
[1] K. Saadian is with the Department of Computer, Babol Branch, Islamic Azad University, Babol, Iran (e-mail: saadyan@yahoo.com).
L. Ajam is with the Department of Computer, Babol Branch, Islamic Azad U/niversity, Babol, Iran (e-mail: leilaajam@yahoo.com).

[۵] نشان دادندکه نرم افزارها ی مخرب RFID، کرم ها ی RFID و ویروس های RFID واقعیت دارد. بدافزارهای RFID می تواند از مؤلفه های سیستم RFID به عنوان مثال بخش مد یریت پایگاه های داده و پروتکل ها ی میان افزار عمومی سوء استفاده کند [۵]. علاوه بر ا ین، حملات مبتنی بر بدافزار بازخوان RFID زمین یک نگرانی جدی است که م ی تواند ارتباط بین بازخوان معتبر و یک تگ را دستکاری کند، خراب کند و برباید [۴].

۳.طرح کلی تکنولوژی RFID

سیستم RFID شامل تگ، بازخوان، و س یستم کامپیوتری (پا یگاه داده بخش مدیریت و برنامه کاربرد ی) می باشد. نمودار جر یان داده RFID در شکل ۱ نشان داده شده است [۳].

تگ وسیله شناسا یی متصل شده به کالا یی است که م ی خواه یم آن را ردیابی کنیم. تگ دارا ی دو بخش تراشه و آنتن م ی باشد که عملکرد ساده ا ی دارد. تراشه اطلاعات را از طر یق آنتن منتشر می کند و حسگرهایی که در ا ین اطراف قرار دارند، اطلاعات را در یافت می‌کنند. بازخوان وسایلی هستند که حضور تگ ها را در محیط تشخیص داده و اطلاعات ذخیره شده در آنها را بازیابی می کنند.



شکل ۱- نمودار جریان داده RFID

أ. تگ ها

با در نظر گرفتن منبع انرژ ی تأمین کننده شان به چهار دسته اصلی تقسیم بندی می شوند:

تگ های غیرفعال: ای نوع تگ ها ه یچ منبع تولید انرژی درونی ندارند و انرژی خود را از طر یق سیگنال‌های RF که توسط بازخوان ارسال و توسط آنتن موجود در تگ دریافت می شود تأمین می‌کنند.

تگ های نیمه فعال: بسیار شبیه تگ ها ی فعال هستند با ا ین تفاوت که باطری کوچکی در آنها وجود دارد و انرژ ی لازم برای فعال شدن مدار داخل آنها را فراهم می سازد.

تگ ها ی فعال: ا ین تگ ها دارا ی یک منبع انرژ ی داخلی می باشند که توانایی انتقال اطلاعات در فواصل دورتر را فراهم می کنند.

تگ ها ی دو طرفه: علاوه بر استفاده از باطر ی داخلی‌شان می‌توانند بدون کمک گرفتن از بازخوان‌ها دیگر اقسام هم شکل خود را زمین شناسایی کرده و با آنها به گفتگو بپردازند.

ب. بازخوان

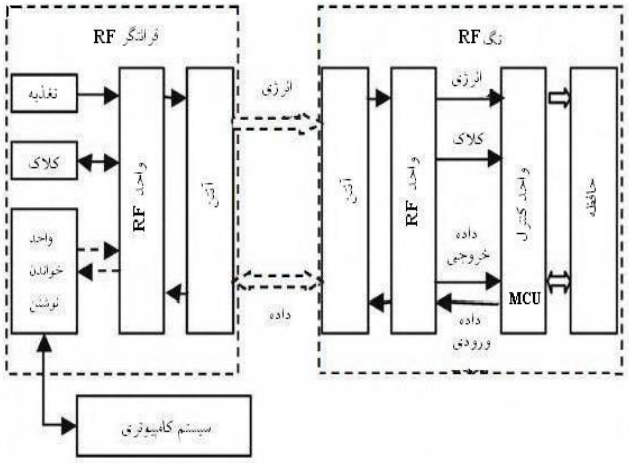
با توجه به هدف و تقس یم بند ی عملکرد به نوع ثابت و نوع قابل حمل ، یکپارچه و گسسته شده است. بر اساس تقسیم فرکانس عملیاتی به چهار نوع فرکانس پایین، فرکانس بالا، فرکانس ها ی فوق العاده (ultra) و مایکروویو تقسیم می شود و براساس الگو ی ارتباط داده می‌تواند به دو طرفه (full duplex) و یک طرفه (half duplex)، دو طرفه متوالی (succession)، یک طرفه و جانشینی تقسیم شود [۲].

ج.آنتن ها

هم در تگ و هم در بازخوان وجود دارد و وظ یفه اصلی آن در یافت و ارسال امواج رادیویی می باشد، به طور ی که دستگاه بازخوان در هنگام خواندن با ارسال سیگنال رادیویی توسط آنتن خود موجب فعال ساز ی تگ می شود و تگ اطلاعات خود را توسط آنتن خود به بازخوان ارسال م ی کند. بزرگی آنتن ارتباط مستقیم با برد آنتن دارد.

د. سیستم کامپیوتری

از اجزا ی د یگر RFID پا یگاه داده و نرم افزارها ی آن می باشد. جهت پشتیبانی اطلاعات از تگ RFID، زمان به محلی برا ی ذخیره و باز یابی اطلاعات است. ای محل توسط نرم افزار ها و پردازشگرها و برقرار ی ارتباط با دستگاههای تگ خوان به استخراج و تبد یل اطلاعات گیرنده‌ها می‌پردازد. بدین ترتیب پس از خواندن کد الکترونیکی محصول توسط بازخوان و ارتباط با پا یگاه داده، امکان بدست آوردن حجم عظیمی از داده های مربوط به آن اطلاعات فراهم می آید.



شکل ۲- سیستم تشخیص فرکانس رادیویی

۴. سیستم RFID، فرمت داده تگ و خطرات امنیتی در بخش مدیریت پایگاه داده

أ. سیستم RFID و فرمت داده تگ

تگ نگهدارنده هو یت منحصر به فرد یک شی است که متشکل از یک آنتن، گیرنده و مدولاتور راد یویی برا ی ارسال پاسخ به بخش مد یریت، منطق کنترلی، مقداری از حافظه و یک سیستم قدرت است[۱]. هر آیتم دارای یک تگ RFID است که شامل یک شناسه منحصر به فرد به نام EPC است و در حافظه آن ذخیره شده است، اطلاعات دقیق آن در بخش مد یریت پایگاه داده قرار شده است، که می‌تواند با توجه به درخواست کاربران نها یی از طر یق رابط کاربر ی که برا ی کاربران ارائه شده است، قابل دسترس ی و مد یریت باشد[۳]. چارچوب معمار ی EPC کاملا مستقل بوده و به صورت ساختار- باز معرفی شده است و مانند

اینترنت قابل توسعه و گسترش می باشد. در استاندارد EPC هر محصول می تواند به صورت منحصر بفرد شماره‌گذاری و شناسایی شود. تعداد رقم‌های هر کد بین ۶۴ تا ۲۵۶ بیت می باشد.

فرمت داده تگ که در جدول ۱ نشان داده شده است، کمک می کند تا برنامه کاربردی، شیء را شناسایی کند. نقشه ساختار هر کد الکترونیکی شامل چهار بخش می باشد: فیلد سرآیند (سرکد)، مدیریت EPC (کد محصول الکترونیکی)، کلاس اشیا و شماره سریال [۱]. فیلد سرآیند طول کلی و فرمت مقادیر فیلد را تعریف می کند. مقدار فیلدها شامل یک شناسه منحصر به فرد EPC است [۲]، و مسئول شناسایی هر شیء که نگهدارنده و تخصیص دهنده کلاسهای اشیاء و کدهای سریال در آن دامنه می‌باشد. هر کلاس شی برای شناسایی یک گروه از اشیا مرتبط می باشد و اشاره دارد به نوع دقیق محصولی که در حال شناسایی است. بنابراین با توجه به مدیر EPC و کلاس اشیا مرتبط، شماره سریال یک عدد منحصر بفرد برای شناسایی هر شی خواهد بود. استاندارد کدگذاری الکترونیکی محصولات [۶] این امکان را فراهم می‌نماید تا برای شناسایی، به هر شی فیزیکی و یا مجازی یک کد منحصر بفرد منتسب نمود.

جدول 1- فرمت داده تگ

شماره سریال	کلاس شی	EPC مدیر	سرآیند

ب. خطرات امنیتی در بخش مدیریت پایگاه داده

خطرات و مشکلات امنیتی عبارتست از جاسوسی یا خرابکاری اطلاعات موجود در تگ ها یا سرورهای اطلاعاتی، یا به نوع ی نشت اطلاعات، دستکاری داده ها، ردیابی‌های مخرب، استراق سمع (رهگیری) می باشد. حملات سیستم RFID که در حال مواجه شدن با آن است متناسب با روش حمله می تواند به دو نوع تقسیم شود: حمله فعال و حمله غیر فعال. هر دوی حملات فعال و غیر فعال مسئله مهم امنیتی سیستم های RFID می باشد که با آن مواجه است. اگر چه حمله غیر فعال در کار عادی سیستم RFID تاثیر نمی گذارد، این رویکرد به طور عمده اطلاعات مربوط به تگ و اطلاعات حساس (نفوذ پذیری) را به دست می‌آورد، در حالی که این مخاطره نباید نادیده گرفته شود[۲]. هنگامی که داده های RFID در مرکز بر روی سرور پایگاه داده ذخیره می شود، هنوز هم از بسیاری از تهدیدات امنیتی و نقطه ضعف هایی رنج می برد. زیرا تگ فقط حاوی یک شناسه است، که آن را به اطلاعات مربوطه پیوند می‌دهد. اگر اطلاعات خوانده شده از تگ به درستی مورد بررسی قرار نگیرد، ممکن است اجرای کدهای تذریق (Injection) SQL که بر روی تگ ذخیره شده است، منجر به تهدید بانک اطلاعاتی شود. تذریق SQL یا ویروس ها، مسائل اصلی در پایگاه داده است. ممکن است پایگاه داده را بدون اطلاع مدیر به کار گیرند. حتی ممکن است رکوردها و یا جداول بدون اطلاع کاربر و یا مدیر مربوطه حذف شوند[۳].

حجم داده ها در تگ می تواند از چند بیت به چند کیلو بایت متغیر باشد. ظرفیت ذخیره سازی تگ برای ذخیره کد ویروس کافی است. یک ویروس RFID یک کد خود تکثیر مستقلی است که نیاز به اتصال به شبکه ندارد. و برای انتشار حمله ویروس کافی است تنها یک تگ RFID آلوده شود. وقتی که یک بازخوان RFID تگ ها را اسکن می‌کند، تگ به ویروس RFID پاسخ می‌دهد، که می‌تواند بخش مدیریت پایگاه داده را آلوده کند [۷]. پس از آن که محتوای تگ‌های به تازگی آلوده شده RFID به عنوان کدهای اجرایی در نظر گرفته شد، ممکن است سیستم های RFID مربوطه را آلوده کند، که منجر به آلوده شدن دیگر تگ ها و دیگر سیستم های نرم افزاری RFID می‌شود [۳].

۵. پیشگیری از بدافزارها در سیستم RFID

در واقع، حمله تذریق SQL یک نوع حمله است که از ورود ی کاربر می‌آید و معتبر بودن آن کنترل نمی شود. یک دستور SQL در پایگاه داده بدون هیچ گونه دانشی از آن درج می شود. تگ ها ی آلوده می توانند با آسیب پذیری سیستم RFID جهت آلوده کردن پایگاه داده عمل کنند. هنگامی که یک ویروس، کرم، یا مخرب دیگر وارد پایگاه داده می شود، تگ ها ی بعدی که با پایگاه داده ارتباط برقرار می کنند نیز ممکن است آلوده شوند، و این خطر ممکن است از طریق عملیات های بعدی گسترش یابد. کرم ها و ویروس های RFID می‌توانند با روش های مختلف توسعه یابند. کرم ها می توانند به عنوان SQL queries روی تگ نوشته شوند، و پس از آن و یروس‌ها تکثیر شوند. در نتیجه، این ویروس ها تهدیدی برای امنیت بخش مدیریت سیستم RFID می باشند که ابتدا در فرم کد وجود دارد، و سپس در بخش مدیریت سیستم از ناحیه داده ها در تگ گسترش می یابد [۳]. اگر اطلاعات تگ دارای ویروس و یا کد حمله باشد، و بخش مدیریت سیستم RFID هیچ مکانیزم ایمنی و یا روشی برای از بین بردن فراهم نکند، باعث می شود کد و یروس به طور گسترده ای انتشار یابد. راه حل برای جلوگیری از این آسیب پذیری، کشف خطر و جلوگیری از اجرای آن است.

أ. یافتن کد تذریق SQL

همان طور که ذکر شد یکی از بدافزارها ، استثمارگر RFID می‌باشد. یک استثمارگر RFID یک داده موجود در تگ می باشد که بخشی از سیستم RFID را که با آن مواجه است مورد بهره بردار ی قرار می دهد. وقتی بازخوان، یک تگ را اسکن می کند، انتظار دارد که اطلاعات تگ را در فرمت معینی دریافت کند. نفوذگر می‌تواند داده‌هایی تولید کند که فرمت و محتویات آن با فرمت مورد انتظار دستگاه بازخوان یکسان نباشد و این باعث می شود که نرم افزار RFID بازخوان و حتی پایگاه داده آن را تخریب کند و یک حمله از نوع وقفه را شکل دهد که باعث می شود شبکه مختل شده و مبادله اطلاعات امکان پذیر نباشد[۷]. سه جنبه کلیدی برای پیدا کردن آسیب پذیری تذریق SQL وجود دارد:۱) شناسایی ورودی اطلاعات پذیرفته شده توسط برنامه کاربرد ی،۲)تغییر دادن مقادیر ورود ی که شامل رشته‌های پر مخاطره (hazardous) می‌باشد، و ۳) تشخیص ناهنجاری‌هایی که توسط سرور بازگردانده شده است [۱].

ب. پیش نمایش کد منبع اتوماتیک

تذریق SQL و آسیب پذیری ویروس به دو دلیل رخ می‌دهد: داده و ساختارهای کنترلی در همان کانال انتقال ترکیب می‌شوند که فاقد صحت ورودی کاربر می باشند. عدم صحت ورودی کاربر به یک مهاجم اجازه دهد تا به یک بخش از داده، مانند یک رشته محصور بین نقل قول و یا یک عدد جهت تذریق دستورات کنترلی و غیره پرش داشته باشد. این دو موضوع منجر به آسیب پذیری پایگاه داده شده است . به منظور جلوگیری در برابر این نوع آسیب پذیری، معیاری برای سنجش صحت ورودی کاربر اتخاذ شده است. به این معنا که تمام ورودی مورد نیاز برای اطمینان از درستی اعلان/ قبل از کدگذار ی به منظور جلوگیری از تذریق SQL مورد استفاده قرار گرفته است [۳].

۶. ملزومات امنیتی RFID

برای محافظت سیستم RFID از بدافزارها، مشخصه های امنیتی که جهت ایجاد داده مطمئن از تگ برای استعلام بین تگ و بازخوان تایید شده است، مورد نیاز می باشد. تکنیک هایی برای تشخیص نرم افزارهایی مخرب از قبیل تجزیه و تحلیل فراخوانی تابع استاتیک روش استخراج داده ها (داده کاوی)، چک کردن مدل وجود دارد[۱].

برای به انجام رساندن امنیت سازی RFID عملیات های مختلف امنیتی و مالکیت حریم خصوصی نیاز است تا با موفقیت اداره شود. غیر قابل ردیابی بودن یکی از آنهاست و احتمالا مهمتر این خاصیت برای حریم خصوصی کاربر است. غیرقابل ردیابی بودن خاصیتی است که مهاجم نمی تواند تگ را با استفاده از فعل و انفعالات با آن، ردیابی کند. ناشناس ماندن تگ خاصیتی است که می تواند از نشت اطلاعات جلوگیری کند.

برای رسیدن به امنیت به بهترین شکل ممکن، پروتکل ها باید اعتبار تگ را برآورده سازند. مانند امنیت رو به جلو (غیر قابل ردیابی رو به جلو)، غیر همگام سازی و انعطاف پذیری [۸]. اولاً نیاز است که از تگ و بازخوان معتبر برای یک تراکنش مطمئن اطمینان حاصل کنیم. ثانیاً مهاجم نتواند داده ها را از طریق رویدادهای قبلی که در آن تگ نقش ی داشته باشد رد یابی کند. حتی اگر مهاجم اطلاعات محرمانه ذخیره شده در تگ را نگهداری کرده باشد[۱].

۷. چارچوب مورد بررسی جهت تایید داده ها و روش احراز هویت

چارچوب مورد بررسی[۱] جهت تضمین امنیت سیستم RFID با استفاده از روش لایه بندی شده در شکل ۳ نشان داده شده است. سه لایه در شکل ۳ وجود دارد. لایه ۱ لایه خواندن داده است که رسانه ارتباط بین خواننده و دنیای خارج خواهد بود. لایه ۲ لایه تایید داده برای بدافزار است. لایه ۳ لایه احراز هویت داده و مونتاژ آن است.

أ. لایه اول

لایه اول بین تگ و لایه های بازخوان ارتباط برقرار می کند. این ارتباط اطمینان حاصل می کند تا داده ها از لایه دوم بگذرد و هم بنطور صحت داده تگ قبل از آنکه به ALE یا سطح نرم افزاری برود تأیید خواهد شد.

ب. لایه دوم

در این لایه یک پایگاه داده کوچک در حافظه بازخوان ذخیره شده است. فرمت پایگاه داده تگ بازخوان در جدول ۲ نشان داده شده است.

جدول۲- پایگاه داده تگ در بازخوان

فایل نامه فرمان SQL	جدول ASCII			کد باینری تگ EPC
	شماره	کاراکتر کنترلی	کاراکتر	

این لایه دو وظیفه اصلی بر عهده دارد:

وظیفه اول: فرمت داده تگ RFID را با استفاده از فیلد کد باینری EPC تگ در پایگاه داده بازخوان پیدا می‌کند. از شماره جهت بررسی صحت محتوا استفاده می کند. در صورت یافت شدن موجودیت کاراکتر، آن را به داده تگ از طریق لایه سوم و لایه اول باز می‌گرداند.

وظیفه دوم: فرمانها ی مخرب در کد شری و مدی EPC را پیدا می‌کند. برای اینکار از فایل نامه فرمان SQL استفاده میکند. هنگامی که یک بازخوان RFID یک برچسب را اسکن می کند، انتظار می‌رود که اطلاعات را با یک فرمت از پیش تعیین شده، دریافت کند. در حالی که یک مهاجم می تواند اطلاعات قلابی را بر روی یک تگ RFID بنویسد، بسیاری غیر منتظره است که فرایند آن، نرم افزار واسطه ای ابتدا و انتها را تخریب نمایی.

استثمارگران RFID اجزا یک سیستم خاص مانند بانکهای اطلاعاتی، ظاهر نرم افزار و کد ها ی نوشته شده را بوسیله مجموعه‌ای از ابزارها ی هک کردن از قبیل پرکردن حافظه، اضافه کردن کد جدید و حملات تذریق SQL هدف قرار می دهند.

یک ساختار مشکل دار می تواند با استفاده از تگ های RFID ارزان قیمت، کارتهای هوشمند بدون تماس یا تجهیزات شبیه ساز برچسبهای RFID حملاتی را هدایت کند.

از دو روش جهت تشخیص صحت داده برای شناسایی کدهای مخرب با توجه به وظیفه اول و وظیفه دوم استفاده می شود:

۱- روش صحت داده جهت شناسایی کدهای مخرب در شماره سریال:

بسیاری از کدهای مخرب به عنوان فرمان مبتنی بر متن در SQL نفوذ پیدا می‌کنند (EXEC و shutdown-- وdrop table). این وظیفه برای روش صحت کد جهت فیلتر کردن کد مخرب در شماره سریال پیاده سازی می شود. برای اینکار ابتدا سرآیند داده در کد با یتری EPC به منظور تعیین فرمت تگ بررسی می شود. بیت های شماره سریال به رشته تبدیل می شود و سپس بیت سریال مرتبط با جدول ASCII را بررسی می کند. در اینجا یک زیر رشته ثابت از تگ به منظور بررسی شماره سریال در جدول ASCII مربوط به پایگاه داده بازخوان در نظر گرفته می شود. اگر الگوریتم 'Accept' را برای تمام داده های سریال برگرداند آنگاه داده تگ برچسب گذاری می‌شود. سپس در این چارچوب سرآیند و سریال برای احراز هویت ارسال خواهند شد. فیلدهای دیگر جهت بررسی صحت در وظیفه دوم بکار گرفته می شود. اگر الگوریتم 'Reject' را برگرداند آنگاه آن داده را رد خواهد کرد.

الگوریتم صحت سریال تگ:

```
Input: tag serial //Binary data
Output: Reject //Boolean (N for Reject, Y=Accept)
Maximum _ length=24 bits // for 64 bit EPC class one tag.
Begin
1. Let aNumbers :{ '0, '1, '2, '3, ….'9}
        //ASCII table of numbers
2. n = minimum_ length_ SQL_SUBSTRING (s_ SQL)
3. read_ tag = tag serial[40rd to 64th bit] // can
   be implemented for 96 bit tag too
4. sSerial = convert_ binary_ to_ string (read_ tag [tag serial
   nth bit])
5. for i = n+1 to maximum_ length
            6. Character_ count = 0
            7. found = search_ substr (sSerial , aNumbers)
            8. if (found==yes)
                    return N
               9. else
                    return Y
               10. cCurrent_ string = convert_ binary_
                   to_ string (read_ tag[i]);
```

```
1. Let  s_ SQL:{‘SHUTDOWN’, ‘DELETE’, ‘INSERT’,
‘EXEC’, ‘DROP’}// SQL command dictionary
2. n= minimum_ length_ SQL_SUBSTRING (s_ SQL)
3. read _tag  = tag data[3rd bit to 40th bit]
4. s_ Text = convert_ binary_ to_ text (read_ tag [first
  nth bit])
5. for i =n+1 to maximum _length Character _count =0
        found= search_ substr (s_ Text, s_ SQL)
        if (found==yes)
      return Y
        else
          return N
        cCurrent _ character = convert_ binary_ to_ text
          (read_ tag [i] );
        s_ Text = s_ Text [2+Character_count to n] +
          cCurrent_ character;
        Character_ count = Character_count+1
6. end for
End
```

اگر الگوریتم 'Accept' را به داده برگرداند آنگاه داده در لایه سوم پردازش خواهد شد.

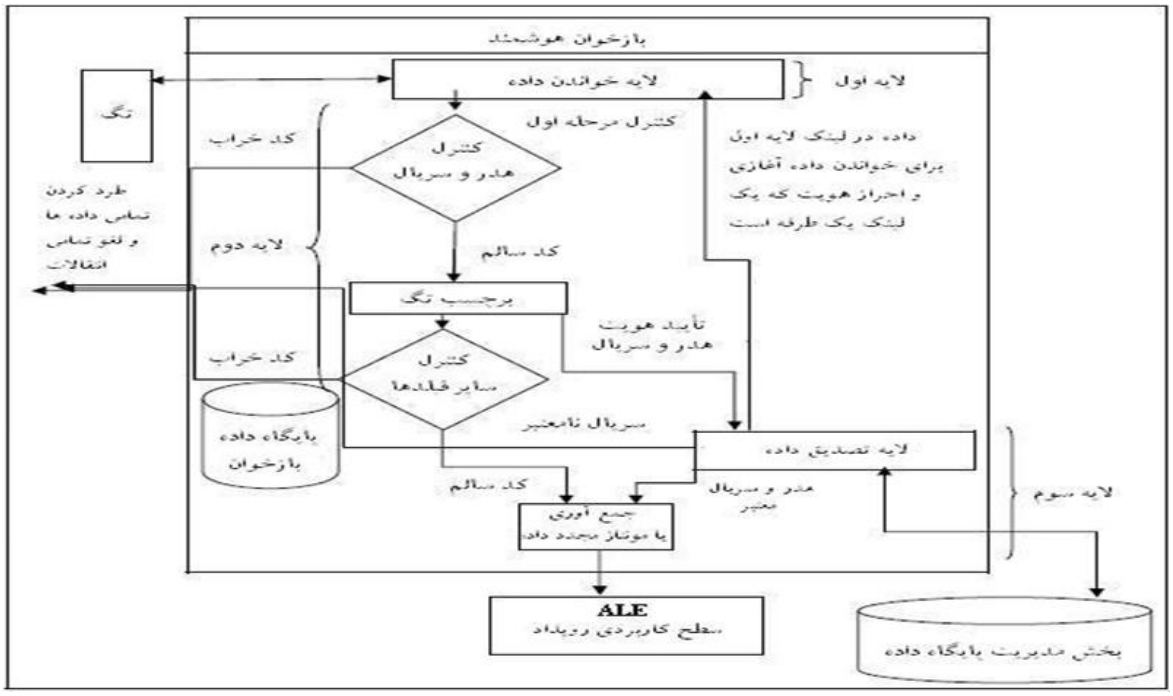
```
11. sSerial = sSerial [2+string_count to
    n] + cCurrent_ string;
12. string_ count = string_count+1
13. end for
14. end
End
```

۲- روش صحت داده جهت شناسایی کدهای مخرب در کد شی تگ و مدیر EPC:

این روش ابتدا کد شی تگ و مدیر EPC را به رشته تبدیل خواهد کرد. اگر رشته تبدیل شده شامل فرمان های مخرب SQL باشد، آنگاه داده تگ مورد نظر رد خواهد شد. در غیر اینصورت آن را برای اسمبل کردن به لایه سوم می فرستد. از فرمت ۶۴ بیتی EPC در این الگوریتم استفاده شده است. در اینجا از یک زیر رشته ثابت از تگ به منظور جستجوی دیکشنری فرمان SQL ذخیره شده در پایگاه داده بازخوان استفاده می شود.

الگوریتم صحت کد شی :

```
Input: tag data //Binary data
Output: Reject //Boolean (Y for Reject, N=Accept)
Maximum _length=38 bits
 Begin
```



شکل۳- چارچوب مورد بررسی جهت تایید داده بازخوان هوشمند و توالی احزار هویت

ج.لایه سوم

این مرحله یک بیت تصادفی و ID بازخوان را با استفاده از تابع Hash صحیح (مبتری بر پروتکل های احراز هویت متقابل) به لایه اول می فرستد. این ها مقادیری هستند که برای شناسایی (احراز هویت) در مرحله بعد استفاده می شود [۹]. در پاسخ به ارسال بیت تصادفی و Hash، تگ یک عدد تصادفی و یک Hash صحیح را به بازخوان، به همراه سایر اطلاعات تگ ارسال می کند. در این دو لایه وظیفه اول فعال می شود. سه مرحله در شناسایی لایه احراز هویت وجود دارد. در پایان فرآیند شناسایی، سرآیند، احراز هویت و شماره سریال،

شناسایی شده و برای دوباره اسمبل شدن به مرحله بعد با داده وظیفه دوم همان برچسب فرستاده می شود.

چارچوب مورد بررسی، حفاظت از بخش مدیریت و حفظ حریم خصوصی تگ را تضمین می کند. این چارچوب در حال کار روی تفکیک داده تگ به منظور کاهش هزینه محاسباتی است. پردازش مواز ی بازخوان بهره وری زمانی را کاهش خواهد داد. احراز هویت داده یک روش شناخته شده برای حفاظت در برابر بدافزارها است. تکنیک تایید داده استفاده شده در این چارچوب از روش جستجوی رشته ا ی با طول ثابت در فایل نامه SQL استفاده می کند که هزینه های ثابت محاسباتی در پی خواهد داشت. به طور معمول به یک حداکثر

هزینه نیاز دارد که متناسب با طول بیت تگ باشد. آن در مقابل، اطمینان از حفاظت از بسیاری از فرمان های دستورات شناخته شده مخربSQL را فراهم می کند. علاوه بر این، می توان پایگاه داده بازخوان را به منظور حفاظت سیستم RFID در مقابل سایر دستورات مخرب سیستمی توسعه داد.

۸. نتیجه‌گیری

بدلیل گسترش سریع سیستم‌های RFID، پتانسیل تهدیدهای احتمالی در آینده بزرگ خواهد بود. این چارچوب مورد بررسی برای محافظت از سیستم RFID در برابر بدافزارها استفاده می‌شود. بهترین حفاظت ممکن در برابر نرم افزارهای مخرب در سطح بازخوان را جهت محافظت از اطلاعات بخش مدیریت برای استانداردهای جهانی EPC ارائه می دهد. به منظور به بینه سازی بهتر، چارچوب های آینده می‌تواند باعث بهبود روش اعتبار سنجی داده‌ها با استفاده از پروتکلهای تایید کننده بین تگ های RFID و نرم افزارهای واسطه ای در این چارچوب شود. تدابیر و تمهیدات امنیتی به طور ذاتی موجب افزایش قیمت تمام شده سیستم خواهد شد که شاید فقط برای سیستم‌ها با حجم بالا و تعداد زیاد اقلام قابل جبران باشد. بنابراین کارهای زیادی در حوزه امنیت و استاندارد سازی سیستم‌های مبتنی بر RFID باید انجام پذیرد.

REFERENCES

1 Shamsul Huda R, Chowdhury MU. Smart RFID Reader Protocol for Malware Detection. 12th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2011; 64-69.

2 Zhenkai W, Zhenkai W. Summarize of RFID Technology and Typical. IEEE Application, 2011; 1032-1036.

3 Li J, Wen J. Security Guarantee in Backend RFID System. International Conference on Business Computing and Global Informatization IEEE Trans., 2011; 55(1): 489-491.

4 Konidala DM. Security Assessment of EPC global Architecture Framework. AUTO-ID Labs, 2006; 13-16.

5 Rieback MR. Pervasive and Mobile Computing. Science Direct, 2006; 405-426.

6 Garfinkel, SL, Juels A, Pappu R. RFID Privacy: An Overview of Problems and Proposed Solutions. Security & Privacy Magazine, 2005; 3(3): 34-43.

7 Rieback M, Simpson P, Crispo B, Tanenbaum A. RFID Viruses and Worms. Department of Computer Science Vrije Universiteit, Amsterdam, 2006.

8 Prenel B. Information Security and Cryptology. 4th International Conference of Information Technology, 2009; 5487

9 Ray S, Chowdhury MU. Enhanced RFID Mutual Authentication Scheme Based on Shared Secret Information. International Society for Computers and Their Applications, 2010.