INT
SCIENCE AND ENGINEERING
1st December 2015 DUBAI - UAE
کنفرانس بین المللی
۱۰ آذرماه ۱۳۹۴ دبی - امارات

تحلیل پروتکل‌های احراز هویت در سیستم‌های RFID

Authentication Protocol In RFID System

فاطمه فتحی سدهی
آدرس پست الکترونیک Gharibeh_fathi@yahoo.com

چکیده

امروزه سیستم‌های RFID برای جمع‌آوری داده‌ها بدون نیاز به دخالت انسان جهت ورود اطلاعات در بسیاری از عرصه‌های صنعتی، علمی، خدماتی و اجتماعی استفاده می‌شود. سیستم‌هایRFID با استفاده از میدان مغناطیسی برای انتقال داده‌ها به‌طور خودکار برای شناسایی و ردیابی تگ‌ها استفاده می‌شود سیستم‌های RFID قادر به تبادل داده‌ها به وسیله برقراری اطلاعات بین یک تگ ،که به یک کالا متصل شده باشد.احراز هویت نقش مهمی در بسیاری از برنامه‌های RFID برای تامین امنیت و حفظ حریم خصوصی دارد. در این پایان‌نامه به تحقیق در رابطه با احراز هویت در سیستم‌هایRFID می‌پردازیم. تاکنون فعالان و محققان در سیستم‌های مختلف به‌دنبال کشف راه‌های حفظ امنیت و حریم خصوصی بوده‌اند.

برای فراهم‌آوردن یک سرویس امنیتی خاص مجبوریم نیازهایی فراهم کنیم. از این رو طرح‌های عملی برای افزایش امنیت و محرمانه‌سازی RFID مطرح می‌شود که از جمله روشهایی مانند توابع چکیده‌ساز و الگوریتم‌های رمزنگاری کلید متقارن و پروتکل‌های احراز هویت می‌باشد. مقاله‌های مختلفی از RFID و روش‌های احراز هویت محصول در زمینه‌های مختلف ارائه شده که در رابطه با آن تجزیه و تحلیل می-کنیم.

واژگان کلیدی: احراز هویت، RFID ، امنیت، حریم خصوصی، پروتکل.

۱- مقدمه

امروزه شناسایی فرکانس رادیویی(RFID)[۱] سیستمی است که از امواج رادیویی برای شناسایی پدیده ها استفاده می‌نماید این سیستم‌ها شامل واحدهای RFID ، امواج رادیویی و بازخوان‌های RFID می‌باشند. بازخوان‌های واحد RFID

[۱] RFID

سیگنال‌های رادیویی را پخش می‌کند تا بدین‌وسیله به داده ذخیره شده در واحدهای RFID دسترسی پیدا کنند. یکی از مهم-ترین تفاوت ها میان بارکدها و واحدهای RFID این است که واحدهای RFID یک شناسه یکتا یا یک اسم مستعار برای هر شیء فراهم می‌کند. استفاده از واحدهای RFID مزایای بسیاری نسبت به بارکدها دارد. به عنوان مثال می‌توان اشاره کرد: داده به صورت خودکار و حتی از طریق یک ماده نارسانا مانند مقوا و کاغذ خوانده شود.

سیستم‌های RFID می‌توانند ابزار ارزشمندی در فرایندهایی مانند ساخت و مدیریت زنجیره تولید واحدهای صنعتی و کنترل انبار باشند. اما، فراگیر شدن سیستم‌های RFID به علت نگرانی در مورد حریم خصوصی افراد و نیز هزینه محدود شده است. از لحاظ اقتصادی می‌بایست هزینه واحدهای RFID سیار اندک باشد که انگیزه کافی برای استفاده از آنها به عنوان جایگزین برای بارکدها وجود داشته باشند.

یک مثال کاربردی دیگر از این فناوری به‌کارگیری آن در سیستم‌های فروشگاهی می‌باشد در این روش به جای بارکد ، روی کالای مختلف یک برچسب ارزان قیمت نصب می‌شود و در خروجی فروشگاه نیز چندین کارت‌خوان یا ریدر نصب می‌گردد، عدم نیاز به دید مستقیم و تماس فیزیکی جهت خواندن برچسب‌ها ، باعث صرفه‌جویی در وقت و جلوگیری از تشکیل صف‌های طولانی در هنگام خروج از فروشگاههای زنجیره‌ای می‌شود، زیرا به جای اینکه تک‌تک کالاها در دید مستقیم توسط دستگاه کارت-خوان بررسی شود و قیمت آن‌ها محاسبه شود ، با یک با عبور سبد پر، از دروازه خروجی فروشگاه که توسط کارت-خوانهای بی‌سیم مجهز شده است و در کسری از ثانیه همهٔ کالاها شناسایی شده قیمت آنها محاسبه می‌شود و صورت حساب تحویل مشتری می‌گردد [۱] .

در این فناوری برای شناسایی اهداف روی هر هدف (کالا، انسان،...) یک برچسب کوچک کار گذاشته می‌شود که این برچسب‌ها حاوی یک شناسه چندرقمی منحصربه‌فرد می‌باشد. هنگامی که یک کالا یا یک هدف مورد نظر در محدوده یا حوزهٔ میدان الکترومغناطیسی کارت‌خوان قرار می‌گیرد ، برطبق یک پروتکل مشخصی که میان برچسب و دستگاه کارت‌خوان کار گذاشته شده یک ارتباط مخابراتی برقرار می‌شود و کارت‌خوان با توجه به شناسه منحصربه‌فرد موجود بر روی یک هدف، آن را به راحتی تشخیص داده و نخستین‌بار ، در جنگ جهانی دوم از فناوری شناسایی از طریق امواج رادیویی استفاده شد. کاربرد این فناوری در شناسایی هواپیمای خودی و دشمن بود که به این کاربرد اصطلاحا" شناسایی دوست یا دشمن (IFF) گفته می‌شود، هنگامی که یک هواپیما در حوزهٔ شناسایی و تشخیص رادارهای خودی قرار می‌گرفت، به کمک سیگنال‌های مشخصی که از هواپیما منتشر می‌شد، رادارها می‌توانستند دوست یا دشمن بودن آن را تشخیص دهند. در دهه‌ی هفتاد و هشتاد میلادی، از این فناوری برای شناسایی گله‌های بزرگ گاو وگوسفند در کشورهای پیشرفته استفاده می‌شد. با پیشرفت چشمگیر فناوری مدارهای مجتمع در ده سال اخیر و در نتیجه کاهش هزینه‌های استفاده از فناوری RFID، شاهد رشد چشمگیری از فناوری RFID در حوزه‌های مختلفی چون بار کدهای الکترونیکی ، بلیط‌های حمل و نقل عمومی، کارت های هوشمند و ... در یک دههٔ اخیر بودیم.

یک سامانه‌ی RFID معمولا" از سه جزء تشکیل شده است:[۲]

- برچسب ها
- کارت‌خوان ها
- سرور یا سرویس‌دهنده مرکزی

نحوه‌ی عملکرد این سامانه‌ها بدین گونه است که به هر برچسب یک شناسه‌ی منحصر به فرد اختصاص داده می‌شود و این شناسه منحصربه‌فرد در حافظه‌ی برچسب ذخیره می‌شود. هر برچسب دارای یک تراشه‌ی بسیار کوچک نیز می‌باشد که ابزارهای محاسباتی و پردازشی در این تراشه واقع می‌شوند. این برچسب‌ها بر روی اهداف مورد نظر برای شناسایی که می‌توانند کالا، انسان و یا حیوان باشند، کارگذاشته می‌شوند. دستگاه‌های کارت‌خوان نیز در مکان‌های مناسبی نصب می‌شوند. کارت‌خوان ها از طریق یک کانال امن که معمولا" کابل است به سرویس‌دهنده مرکزی متصل می‌شوند. در سرویس-دهنده مرکزی نیز اطلاعات مربوطه به همه‌ی برچسب‌ها در یک حافظه‌ی امن و بزرگ ذخیره می‌شود. برای مثال اگر فرض کنیم که اهداف مورد برای احراز هویت، کارت‌های شناسایی مربوط به افراد یک سازمان باشند، آن‌گاه اطلاعات هر فرد شامل نوع نام، نام‌خانوادگی، پست‌سازمانی، مکان‌های مجاز برای دسترسی این فرد، تاریخ انقضای کارت... و به همراه شناسه‌ی منحصر به فردی که روی برچسب آن کارت ذخیره شده است، در سرویس‌دهنده مرکزی ذخیره می‌شود. برای تک‌تک افراد، این اطلاعات در درایه‌هایی مشخصی ذخیره می‌شود. هنگامی که یک فرد به همراه کارت خود در حوزه‌ی میدان مغناطیسی یک کارت‌خوان قرار بگیرد، برطبق یک پروتکل ارتباطی مشخص، بین یک برچسب و کارت‌خوان اطلاعاتی ردو بدل شده و بر چسب می‌تواند شناسه‌ی انحصاری خود را برای کارت‌خوان، به صورت بی‌سیم ارسال کند. به محض دریافت هر شناسه، سرویس‌دهنده در بین همه‌ی شناسه‌های موردنظر، اطلاعات مربوط به آن را استخراج کرده و آن‌ها را روی خروجی می‌فرستد. به این‌ترتیب در کسری از ثانیه فرد مورد نظر شناسایی شده و اطلاعات مرتبط با آن نیز استخراج می‌شود ، بدون آنکه نیاز به تماس فیزیکی و مستقیم وجود داشته باشد.

هر چند استفاده از سامانه ی RFID روزبه‌روز در حال گسترش است و هر روز به تعداد کاربران این سامانه ها اضافه می‌شود، با این‌حال استفاده از این سامانه‌ها با چالش‌های امنیتی عمده‌ای نیز روبرو است، برای تامین امنیت یک سامانه‌ی RFID در لایه‌ی پروتکل، تنها ابزاری که می‌تواند به کارگرفته شود پروتکل تصدیق اصالتی است که بین برچسب و کارت‌خوان اجرا می-شود و در حین اجرای آن، طرفین هویت یکدیگر را بررسی کرده و در صورت صحت می‌پذیرند. به دلیل آن که یک برچسب RFID باید با کم‌ترین هزینه تولید شود، در نتیجه امکان استفاده از توابع رمزنگاری قدرتمند روی برچسب‌ها وجود دارد و در نتیجه امکان استفاده از توابع رمزنگاری قدرتمند روی برچسب‌ها ی RFID وجود ندارد و فقط امکان پیاده سازی اولیه‌هایی همچون شکل ساده شده‌ای از توابع درهم‌ساز، مولد اعداد شبه تصادفی و عملگرهای منطقی هم‌چون OR , AND, XOR, و عملگرهای مشابه روی برچسب‌ها وجود دارد، در نتیجه پروتکل‌های امنیتی طراحی‌شده برای این سامانه‌ها باید با در نظرگرفتن همه‌ی این محدودیت‌ها طراحی شوند.

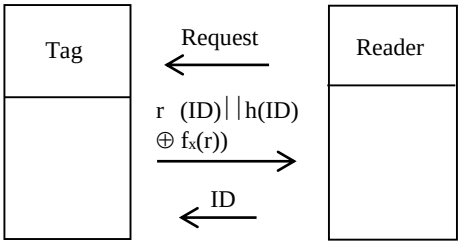
۲- مروری بر پروتکل ها

در سال‌های گذشته، پروتکل‌های احراز هویت بسیاری جهت به کارگیری در سامانه‌های RFID مطرح شده‌اند. که هر کدام دارای نقاط ضعف و قوت بوده‌اند و مقاله‌های زیادی منتشر شده است که ضعف‌های آن ها را نشان داده‌اند، با این وجود هنوز چالش بر سر دستیابی به یک پروتکل که همه‌ی ملزومات امنیتی مورد نیاز را فراهم کند ، ادامه دارد. در پایین به بعضی از پروتکل‌های احراز هویت در سیستم‌های RFID اشاره خواهیم کرد.[۳،۴،۵،۶]

در میان این پروتکل‌ها، یکی از قدیمی‌ترین پروتکل‌ها را ویس و همکارانش پیشنهاد دادند،[۷] مقیاس زمانی از بالا به پایین می‌باشد. این امر بدین معنا است که بالاترین پیام اول فرستاده می‌شود و پایین‌ترین پیام در آخر فرستاده می‌شود. عملگرهای الحاق و عملگرهای منحصربفرد (OR) (یا XOR) به ترتیب بصورت || و ⊕ نشان داده می‌شوند.

در اینجا، fx(r) یک مجموعه از شبه تابع تصادفی است. هم تگ و هم ریدر دارای رمز (x) هستند. این پروتکل در مقابل حمله-ی مجدد مهاجم ایمن نیست. مثلاً مهاجم می‌تواند پیام‌های بین تگ و ریدر را استراق سمع کند و آنها را ثبت نماید. در زمان-

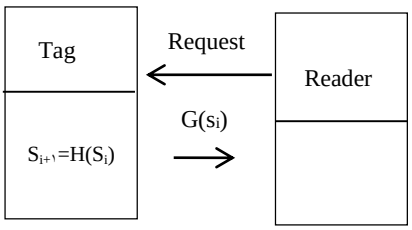
های بعدی مهاجم می‌تواند پیام تگ به ریدر را تکرار کند و ریدر آن را به عنوان یک تگ معتبر می‌پذیرد، یعنی مهاجم قادر است تگ را برای یک ریدر قانونی جعل کند.
می‌توانیم حمله‌ی مجدد را دشوارتر سازیم، بدین‌صورت که بگذاریم ریدر(r) را تولید کند و آن را همراه با پاسخ ارسال نماید. حملات مجدد وقتی نسبتا دشوار می‌شوند که مقادیر تصادفی جدید در حین هر فرآیند جدید احراز هویت تولید می‌شوند و بکار می‌روند. آسیب‌پذیری دیگر به انتشار آزاد شناسه‌ی (ID) تگ بر می‌گردد. مهاجم می‌تواند از آن برای ردیابی تگ‌ها استفاده کند.



شکل (۱): پروتکل ویس و همکارانش[۷]

مشابه پروتکل قدیمی بعد از پروتکل ویس ، سارما، ریوست و پروتکل اهکوبو، سوزوکی و کینوشیتا می‌باشدکه برای یک تگ مجزای RFID است. شکل (۲) زیر طرح اولیه این پروتکل را نشان می‌دهد ، این پروتکل بر دو زنجیره‌ی درهم‌سازی (G و H) تکیه می‌کند تا یک شناسه‌ی تصادفی که هم در تگ و هم در پایگاه داده‌ی سیستم ذخیره می‌شود را بروز برساند. که در این پروتکل هم از تابع هش و هم از مولد اعداد تصادفی استفاده می‌کند، شناسه‌ی تصادفی با (s_1) شروع می‌شود.
وقتی ریدر به تگ پاسخ می‌دهد، تگ $G(s_i)$ را محاسبه می‌نماید و آن را برای ریدر ارسال می‌کند، سپس با استفاده از تابع درهم‌سازی دیگر ($H(S_{i+1})=H(s_i)$)، شناسه را بروز می‌کند. پایگاه داده‌ی بخش مدیریت که به ریدر متصل است جفت‌های (ID^k , S^k) را حفظ می‌کند، (ID^k) عبارت است از شناسه و (S^K) عبارت است از اطلاعات محرمانه‌ی اولیه برای تگ (k) می-باشد. [۸]

از این رو مهاجم در حمله به این پروتکل باز می‌ماند، چون اطلاعات استفاده شده در این پروتکل بروز می‌شود و چون این اطلاعات توسط تابع در هم‌ساز هش پیچیده‌تر شده مهاجم بسیار مشکل بتواند به این اطلاعات دسترسی داشته باشد. هرچند این پروتکل در برابر حملات مجدد ایمن نیست. مثلاً یک مهاجم می‌تواند درخواستی را برای تگ ارسال کند و پاسخش را ثبت نماید و مدتی بعد بدون حضور تگ آن را برای ریدر تکرار کند.



شکل۲: پروتکل از اهکوبو ، سوزوکی و کینوشیتا [۸]

در سال (۲۰۱۲) Yun-Tian و همکارانش یک پروتکل فوق سبک وزن جدید به نام (RFID Authentication Protocol With Permutation)(RAPP) پیشنهاد کردند. در این پروتکل Tag یا برچسب توانایی انجام سه عملیات را دارد: (عمل XOR ، عمل گردش به چسب، و تابع جایگشت) که تمامی این عملیات بر روی برچسب‌های ارزان قیمت قابل پیاده‌سازی می-باشد. در این پروتکل یک کانال ارتباطی بین ریدر و سرور امن و کانال بین ریدر و برچسب نا امن فرض شده است. هر برچسب دارای یک شناسه یکتای L بیتی (ID) و مقادیر محرمانه (ID_S, K_1 , K_2 , K_3) می‌باشد، در این پروتکل در پایان هر نشست موفق مقادیر به‌روزرسانی می‌شود. به منظور جلوگیری از حمله نا همزمانی مقادیر قدیم و جدید کلیدهای مشترک در برچسب، در سمت سرور ذخیره می‌شود.[۹]

در این پروتکل از تابع جدیدی به نام Permutation یعنی همان تابع جایگشت استفاده شده است، که عملکرد این تابع به شکل زیر می‌باشد.

برای روشن‌شدن این موضوع مثال زیر را مرور می‌کنیم:

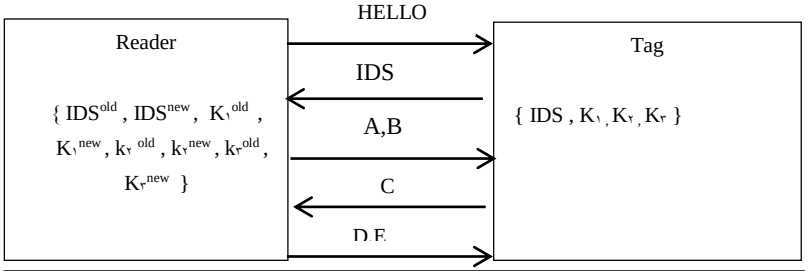
X = ۰۱۱۱۰۱۱۰۱۰۱۰۱۱۰۱

Y = ۱۱۰۱۰۱۱۱۱۰۱۱۰۰۰۱

که جایگشت X نسبت به Y :

Per (x, y) = (۰۱۱۱۱۰۱۰۱۰۱۱۰۰۱)

همانطور که بالا مشاهده می‌کنید، در این تابع چنانچه بیت اول رشته عملگر دوم (Y) صفر باشد اولین بیت عملگر اول (X) در انتها رشته خروجی قرار می‌گیرد و چنانچه بیت اول رشته (Y) یک باشد بیت اول رشته (X) به عنوان اولین مکان در رشته خروجی قرار می‌گیرد و این روند تا انتهای رشته‌ها تکرار می‌شود. و این ترتیب کار زمانی که انجام شد می توانید از این ترکیب در پروتکل پایین به راحتی استفاده کنید.



A= per (k_2,k_1) ⊕ n_1

B= per (k_1 ⊕ k_2,Rot (n_1, n_2)) ⊕ per (n_1 , k_1)

شکل(۴) : مراحل پروتکل RAPP

۳- پروتکل کال آواستی

تگ معمولاً بر روی شیء قرار داده می‌شود و دارای مقادیر شناسایی مثل کلید مخفی و یک شناسه است که در حافظه‌اش ذخیره شده. این مقادیر همچنین در سرور ذخیره می‌شوند و تگ می‌تواند با ارسال و دریافت این مقادیر در سرور از طریق یک ریدر هویت خود را احراز کند.

ریدر با ارسال سیگنال‌های فرکانس رادیویی (RF) در مورد مقادیر شناسایی هویت تگ ها پرسش می‌کند تا هویت آنها را احراز نماید. این پیغام‌ها از طریق هوا در سیستم‌های RFID منتقل می‌شوند و این پروتکل‌ها در مرحله‌ی احراز هویت هنوز به طور مستقیم از شناسایی واقعی تگ‌ها مثل شناسه‌ی تگ و کلید مخفی استفاده می‌کنند. برای این منظور، کاربران RFID می‌توانند محتوای تگ‌های RFID را برای عموم منتشر سازند زیرا هر ریدر مخرب RFID می‌تواند مکان آنها را شناسایی کند یا بین شناسایی و اطلاعات خصوصی آنها تمایز قائل شود. در این پروتکل با اضافه کردن توابع جدید، مسائل امنیتی و حفظ حریم خصوصی را ارتقا می‌دهند.[۱۶]

نمادها و سمبل‌های استفاده شده در پروتکل کال و آواستی

Tid_i = شناسه ی تگ	&T = تأخیر پیش‌بینی شده‌ی انتقال
K_i = کلید مخفی تگ	T_{tag} = زمان فعلی در تگ
s_i = مقدار مخفی تگ	T_{reader} = زمان فعلی در ریدر
tid_i^{new} = شناسه‌ی جدید تگ	T_{server} = زمان فعلی در سرور
k_i^{new} = کلید مخفی جدید تگ	h() = تابع درهم‌ساز (هش)
s_i^{new} = مقدار مخفی جدید تگ	$\oplus$ = عملیات XOR بیتی
r_1, r_2 = اعداد شبه تصادفی	$\|\|$ = عملیات الحاق و ترکیب

شکل(۴):نمادهای پروتکل کال آواستی(۱۶)

دو مرحله از احراز هویت RFID که عبارتند از مراحل مقداردهی اولیه و پایان‌دهی که با احراز هویت تگ و سرور بدون استفاده از مقادیر واقعی تگ (کلید مخفی و شناسه) ، امنیت و حفظ حریم خصوصی RFID را ارتقا می‌دهد. پس از اینکه تگ و سرور به طور موفقیت‌آمیز مرحله‌ی را طی کردند، مرحله‌ی تضمین می‌کند که سرور اطلاعاتی در مورد وضعیت احراز هویت و بروزرسانی تگ دارد. درادامه بصورت زیر سازماندهی شده است.

پروتکل کال و آواستی همراه با دو مرحله‌ی پیشنهادی به عنوان مثال از پروتکل‌های احراز هویت قبلی استفاده می‌کنیم. کال و آواستی برای جلوگیری از قابلیت ردیابی تگ با بروزرسانی کلید مخفی تگ (k_i) و شناسه (tid_i) بین تگ و سرور، یک پروتکل احراز هویت را پیشنهاد دادند. آنها از تابع درهمسازی یک طرفه، مولد اعداد شبه تصادفی و عملیات XOR بیتی استفاده کردند تا تمام عملیات در پروتکل را محاسبه نمایند، پروتکل آنها شامل سه مرحله بود:

- مرحله‌ی مقدار دهی اولیه
- مرحله‌ی احراز هویت
- مرحله‌ی بروزرسانی

در مرحله‌ی مقداردهی اولیه، هویت تگ و کلید مخفی تگ (tid_i , k_i) بوسیله‌ی سرور تعیین شده و در حافظه‌ی تگ و سیستم پایگاه داده ذخیره می‌شوند. ریدر هیچ اطلاعاتی در مورد این داده ها ندارد. به همین ترتیب، سرور جفت جدید شناسه‌ی تگ و کلید مخفی تگ (tid_i^{new}, k_i^{new}) را در پایگاه داده ذخیره می‌کند .[۱۷]

در مرحله‌ی احراز هویت، عدد شبه تصادفی r_1 از ریدر به تگ ارسال می‌شود. سپس ، تگ r_2 را تولید می‌کند و پیغام های (A_1) و (A_2) را محاسبه می‌کند:

$A_1 = h(k_i \oplus r_i) \oplus r_2$

$A_2 = h(tid_i \| r_1 \| r_2 \| k_i \| T)$

تگ پیغام A_1، A_2 و T (زمان فعلی تگ) را به ریدر ارسال می‌کند، تا آن را مجدداً به سرور ارسال نماید. وقتی ریدر پیغام (A_1, A_2, T) را دریافت می‌کند، با مقایسه‌ی زمان فعلی ریدر (T') با زمان تگ:

$(T' - T) \leq \&T$

در نهایت برچسب زمان را بررسی می‌کند ، یعنی در جایی که انتظار می رود $(\&T)$ بازه‌ی زمانی برای تأخیر انتقال باشد. اگر درخواست احراز هویت پذیرفته شود، ریدر زمان پیغام را با زمان ریدر تعویض می‌کند و پیام (A_1, A_2, T') را به سرور ارسال می‌نماید، حالا در غیر این‌صورت، ریدر درخواست احراز هویت را رد می‌کند. همچنین، سرور برچسب زمان را با زمان فعلی $(T'' - T') \leq \&T$ سرور تأیید می‌کند، اگر درخواست احراز هویت پذیرفته شود، سرور به دنبال (r_2^*) خواهد بود تا (A_2^*) را محاسبه کند.

(A_2^*) را با (A_2) دریافت شده از تگ مقایسه نماید، یعنی:

$r_2^* = A_1\, h(k_i \oplus r_1)$

$A_2^* = h(tid_i \| r_1 \| r_2^* \| k_i \| T'')$

در غیر این‌صورت، سرور درخواست احراز هویت را رد می‌کند. پس از احراز هویت تگ در سرور، سرور(A_3) را محاسبه کرده و آن را از طریق ریدر به تگ ارسال می کند.

$A_3 = h(tid_i \oplus r_1 \oplus r_2 \oplus k_1)$

ریدر آن را مستقیماً به تگ ارسال می‌کند، سپس تگ $(A3)$ را محاسبه کرده و آن را با پیغام A۳ ، مقایسه می‌کند تا احراز هویت متقابل را تکمیل نماید.

در مرحله‌ی بروزرسانی، تگ(tidi و ki) را بروز می‌کند و آنها را با شناسه‌ی جدید و کلید مخفی تگ جایگزین می‌کند یعنی:

$(tid_i^{new}) = (tid_i \oplus r_1 \oplus r_2) \,\&\, k_i^{new})$

از طرف دیگر ، سرور آنها را جایگزین نمی‌کند ، اما تا زمانی که تکمیل احراز هویت کامل نشود ، شناسه‌های قدیمی و جدید و کلیدهای مخفی تگ را حفظ می‌کند.

مرحله ۱: ریدر← تگ

ریدر عدد تصادفی (r_1) را تولید کرده و آن را به تگ ارسال می‌کند.

مرحله ۲: تگ ← ریدر

در این مرحله، از تابع درهمسازی ساده همراه با مقدار مخفی(s_i) استفاده می‌کنیم. تگ (r_2) را تولید می‌کند و دو عدد تصادفی r_1 و r_2 با یکدیگر در یک پیام به شکل $x= (r_1 \| r_2)$ قرار خواهند گرفت .پیغام x به مقدار (s_i) الحاق می‌شود یعنی ($x \| s_i$) ، و سپس از تابع درهمسازی استفاده می‌کنیم، به گونه‌ای که به $h (x \| s_i)$ را داشته باشیم. پس از آن، را محاسبه می‌کند و سپس $h(x \| s_i)$ و (y) را همراه با زمان فعلی تگ یعنی $(h(x \| s_i) , y, T_{tag})$ به ریدر ارسال می‌کند .

پس از ارسال پیام، تگ منتظر پیام «Hello (سلام)» می‌ماند تا فرآیند احراز هویت زیر را با کلید مخفی واقعی و شناسه‌های تگ آغاز کند.

مرحله ۳: ریدر⟵ سرور

پس از دریافت پاسخ تگ،ریدر با مقایسه‌ی زمان فعلی ریدر(T_{reader}) با زمان تگ $(T_{reader} - T_{tag}) \leq \&T$ زمان پیغام را تأیید می‌کند. اگر پیغام پذیرفته شود، ریدر r_1 را اضافه می‌کند و زمان پیغام را با زمان ریدر تعویض کرده و پیغام $(r_1 , h(x \| s_i) , y , T_{reader})$ را به سرور ارسال می‌کند.

مرحله ۴: سرور

پس از دریافت پیغام از ریدر، سرور با مقایسه‌ی زمان فعلی سرور (T_{server}) با زمان ریدر$(T_{server} - T_{reader}) \leq \&T$، زمان پیغام را تأیید می‌کند. اگر پیغام پذیرفته شود، سرور با مقایسه‌ی y، به دنبال *r۲ می‌گردد. سپس، سرور این پیغام $(h (x \| s_i) , y , T_{reader})$ را در یک سری سه مرحله‌ای تأیید می‌کند. اول اینکه سرور، $h(x \| s_i)$ را از پیغام دریافتی استخراج و ذخیره می‌کند. دوم اینکه سرور پیغام $x =(r_1 \| r_2*)$ را به مقدار s_i در تگ ذخیره شده در سرور الحاق کرده و از تابع درهمسازی بر روی آنها استفاده می‌کند. در آخر، سرور پیغام درهمسازی شده‌ای که در سرور محاسبه شد را با پیغام محاسبه شده در تگ مقایسه کرده و اگر آنها برابر باشند، سرور پیغام (Hello) را برای شروع فرآیند احراز هویت ارسال می‌کند. اگر این پیغام‌ها برابر نباشند، سرور این فرآیند را قطع می‌کند.

مرحله‌ی پایانی احراز هویت:

مرحله ۵: تگ ⟵ ریدر

ایده‌ی اصلی ارسال مجدد یک پیام درهمسازی شده در این مرحله تضمین این مسئله است که سرور از وضعیت تگ آگاه است، یعنی آیا پیغام (A_3) پذیرفته‌شده و مقادیرش بروز شده‌اند یا اینکه پیغام (A_3) به تگ نرسیده است. اگر سرور این پیغام را دریافت کند، یعنی تگ اکنون معتبر است و مقادیرش بروز می‌شوند، در غیر این‌صورت، سرور مقادیرش را بروز نکرده و در عوض قطع می‌شود. بنابراین، وقتی تگ پیغام A_3 را می‌پذیرد، این پیغام $(h(x \| s_i) , T_{tag})$ را به سرور ارسال می‌کند و به مرحله‌ی بروزرسانی وارد می‌شود، در غیر این صورت قطع می‌گردد.

مرحله ۶: ریدر ⟵ سرور

ریدر زمان پیغام را تأیید کرده و پس از تایید آن را به سرور منتقل می‌کند.

راهکارهای حفظ حریم خصوصی:

مشکل اصلی در حفظ حریم خصوصی در سامانه‌ی RFID نشست اطلاعات محرمانه از برچسب است، بهترین راه‌کار برای تامین امنیت خصوصی استفاده از پروتکل‌های احراز هویت می‌باشد، هدف از این پژوهش، تحلیل، طراحی و بهبود امنیتی پروتکل احراز هویت در سامانه‌ی شناسایی اجسام توسط (RFID) می‌باشد، یک پروتکل با راهکارهای امنیتی بسیار بالا در برابر یک مهاجم، واستفاده مفید و آسان از این تکنولوژی RFID می‌باشد، با استفاده از ارائه پروتکل‌های احراز هویت مناسب RFID ، می‌توان در این راه گام بزرگی برداریم.

٤- طرح پیشنهادی:

این پروتکل دارای یک مرحله‌ی مقدماتی است که در آن برچسب‌ها و سرویس‌دهنده یک مقدار اولیه می‌گیرند و یک مرحله‌ی احراز هویت دو طرفه دارد که طرفین هویت یکدیگر را بررسی کرده و در صورت صحت یکدیگر را می‌پذیرند. در طراحی یک سیستم نیازمند این است که به طورخاص ، باید مجموعه‌ای از ارتباطات RFID ، با یک پروتکل امن پیاده سازی شود. معمولاً، تعداد زیادی تگ RFID وجود دارد که هویت آنها باید در محیط یک ریدر احراز هویت شود. عملکرد این پروتکل و احراز هویت آن را با اجزاء و المان های داخلی آن با رسم دیاگرام توضیح می‌دهیم.

در این پروتکل به جای استفاده از ترکیبات الحاقی از تابع جایگشت استفاده می‌کند که تابع جایگشت تابع قوی‌تری نسبت به تابع الحاقی می‌باشد عملکرد دقیق‌تر این تابع در بالا شرح داده شده است، این تابع جایگشت با استفاده از (XOR) می‌تواند پیوند محکمی در نگهداری خوب توابع باشد.

در مرحله‌ی مقداردهی اولیه، سرور ابتدا شناسه‌ی تگ (tid_i)، کلید مخفی تگ (k_i)، مقدار مخفی تگ (x_i)، را تعیین می‌کند و در حافظه‌ی تگ و پایگاه داده سرور ذخیره می‌کند. در مرحله‌ی بعدی ریدر عدد تصادفی (n_1) را تولید کرده است و آن را به تگ ارسال می‌کند. در مرحله‌ی بعدی از تابع در هم‌ساز KECCAK استفاده می‌کنیم، این تابع نسبت به توابع درهم-ساز دیگر پیچیده‌تر و قوی‌تر می‌باشد. در این پروتکل از دو مرحله یک مقداردهی اولیه و دیگری پایان‌دهی آن می‌باشد که همراه با احراز هویت تگ و سرور به طور موفقیت آمیزی مرحله را طی می‌کند.

این مراحل با استفاده از توابع درهم‌ساز و عملیات (XOR) و تابع جایگشت می‌تواند تا حدودی امنیت و حفظ حریم خصوصی RFID را ارتقاء ببخشد.

در مرحله‌ی احراز هویت، عدد شبه تصادفی(n_1) از ریدر به تگ ارسال می‌شود، سپس ، تگ (n_2) را تولید می‌کند و پیغام‌های (C_1 و C_2) تولید می‌شود و تگ پیغام که حاوی محتوی که در حقیقت زمان فعلی تگ می‌باشد را به ریدر ارسال می‌کند و سپس ریدر آن را به سرور ارسال می‌کند و آن ها از طریق همین مقایسه زمانی‌ها می‌توانند برچسب زمانی را بررسی کنند.

در این مرحله، از تابع درهمسازی ساده همراه با مقدار مخفی (x_i) استفاده می‌کنیم. تگ (n_2) را تولید می‌کند و دو عدد تصادفی (n_1وn_2) با یکدیگر در یک پیام به شکل ($f=per(n_1, n_2)$) قرار خواهند گرفت.

step[۱] پیغام (f) به مقدار (x_i) جایگشت می‌شود یعنی (per (f , x_i)) و به گونه‌ای که به این KECCAK (per(f, x_i) را داشته باشیم. پس از آن، تگ ($m= x_i \oplus n_2$) را محاسبه می‌کند و سپس (KE (per(f, x_i)) و (m) را همراه با زمان فعلی تگ یعنی (K(per(f, x_i)) , y , T_{tag}) به ریدر ارسال می‌کند.

در پروتکل پیشنهادی بالا همانند پروتکل‌های احراز هویت دارای یک سری اصول ارسال و ثبت اطلاعات می‌باشد، ابتدا ریدر عدد تصادفی(n_1) را تولید می‌کند. این عدد تصادفی را به تگ می‌فرستد تگ پس از دریافت عدد تصادفی تولید شده، عدد تصادفی (n_2) را تولید می‌کند و این دو عدد تصادفی را با تابع جایگشت (Permutation) ترکیب کرده و با نام تابع (f) نگهداری می‌کند و سپس مقدار مخفی تگ (x_i) و (f) را با استفاده از تابع درهم ساز مستحکم Keccak می‌زنیم.

همراه با مقدار مخفی تگ که باید با استفاده از توابع (XOR) به صورت نامفهوم در می‌آوریم یعنی مقدار مخفی را با عدد تصادفی تگ (XOR) می‌کند و بعد با نام تابع (m) به ریدر می‌فرستد و ریدر نیز زمان فعلی خودش را و تگ را از هم کم می‌کند و همان پارامترها را با عدد تصادفی خود ریدر به سرور می‌فرستد و سرور باز زمان فعلی خودش و ریدر را مقایسه می‌کند و می‌آید عدد تصادفی تگ را خودش محاسبه میکند.

یعنی وقتی (طخق) میشود تابع مقدار داخلی آن یعنی (n_2) را باز یابی می‌کند و سپس خود سرور می‌آید این تابع (f) و مقدار مخفی تگ (x_i) را با تابع جایگشت بدست می‌آورد سپس با تابع کچک درهم‌ساز می‌کند اگر مقدار دریافتی با مقدار ارسال شده از ریدر یکی باشد به این مفهوم تگ مورد نظر معتبر می‌باشد بنابراین مرحله‌ی احراز هویت آغاز می‌شود و پیام را ارسال می-کند. و پس از آن به این شکل که می‌آید (m) و مقدار مخفی تگ را که در سرورها از قبل ذخیره شده‌اند را بازیابی می‌کند.

در پروتکل پیشنهادی برای بالا رفتن امنیت بیشتر سیستم از توابع هش (KECCAk)۲۰۱۳ استفاده کرده ، که علاوه بر این در این پروتکل در زمان احراز هویت پیام‌های (C_1) و (C_2) را ترکیب الحاقی کنیم در این صورت احتمال انجام حمله در این پروتکل‌ها بسیار کاهش می‌یابد و چون مهاجم به راحتی نمی‌تواند در یک مرحله شنود به اطلاعات دسترسی داشته باشد.

۵- نتیجه‌گیری

با گسترش روزافزون این فناوری و با توجه به نیاز استفاده بشر از این فناوری نیازمند این هستیم که در تامین امنیت و حفظ حریم خصوصی این فناوری راهکارهایی را اندیشیده باشیم، از این حیث مفهومی که در این فناوری به دنبالش هستیم که این سیستم ها را با بهای ارزان بتوانیم در اختیار مصرف‌کنندگان قرار دهیم از این رو اگر از الگوریتم‌های رمزنگاری در این سیستم ها بخواهیم استفاده کنیم، قیمت این فناوری افزایش پیدا می‌کند پس مستلزم استاده از پروتکل‌های احراز هویت قوی می‌باشد که در مقابل یک مهاجم بیشترین مقاومت را از خود نشان دهد، ما می‌توانیم با استفاده از پروتکل‌هایی که ایمن‌تر هستند و استفاده از عملیات‌های منطقی و ریاضی و پیچیده‌ترکردن آن‌ها، در هرچه امن‌تر نگه‌داشتن این سیستم‌ها قدمی نهادینه کنیم.

۶- مراجع

[۱] J.Banks, M. Pachano. L. Thompson, and D. Hanny, "RFID applied", JOHN WILY & SONS, Inc, ۲۰۰۷.
[۲] G. Roussos, "Networked RFID: Systems, software and services", Springer- Verlag London, Computer communications and networks series, ۲۰۰۸.
[۳]P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez- Tapiador, and A. Ribagord, "LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags", In: Proceedings of the ۲nd Workshop on RFID Security, July ۲۰۰٦.
[٤] H. Y. Chien and C. H. Chen, (۲۰۰۷), "Mutual authentication protol for RFID conforming to EPC class ۱ generation ۲ standards", Computer Standards & Interfaces, ۲۹(۲), ۲٥٤-۲٥۹. Dio:۱۰,۱۰۱٦/j.csi.۲۰۰٦,۰٤,۰۰٤.
[٥] J. Fu,C. Wu, X. Chen, R. Fan and L. Ping, "Scalable pseudo random RFID private mutual authentication" , ۲۰۱۰ ۲nd International Conference on Computer Engineering and Technology(ICCET). Chengdu, China. April, ۲۰۱۰, V. ۷, pp.٤۹۷-٥۰۰.
[٦] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, "Lightweight mutual authentication and ownership transfer for RFID systems", In Proceedings of IEEE INFOCOM ۲۰۱۰, San Diego, CA, (۲۰۱۰) ۱-٥.
[۷] S.A. Weis, S.E. Sarma, R. Rivest, D.W. Engels, Security and privacy aspects of low-cost radio frequency identification systems, Proceedings of the ۱stSecurity in Pervasive Computing, LNCS, vol. ۲۸۰۲, ۲۰۰٤, pp. ۲۰۱_۲۱۲.
[۸] M. Ohkubo, K. Suzuki, S. Kinoshita, A cryptographic approach to a 'privacy-friendly' tags, RFID Privacy Workshop, MIT, November ۱٥ ۲۰۰۳.
[۹] Yun Tian, Gongliang chen, "A new ultra-lightweight RFID Authentication protocol permutation" IEEE Communication Letters, Vol.۱٦.No, ٥, May ۲۰۱۲.
[۱۰] Kaul SD, Awasthi AK. RFID authentication protocol to enhance patient medication safety. Journal of medical systems, ۳۷(٦). ۲۰۱۳.p. ۱-٦.
[۱۱] Stallings W. Cryptography and network security, principles and practices. Practice Hall. ۲۰۰٦.
[۱۲] Chien HY. SASI: A new ultra-lightweight RFID authentication protocol providing strong authentication and strong integrity. Dependable and Secure Computing, IEEE Transactions on. ۲۰۰۷. P. ۳۳۷-۳٤۰.