TEEGES

Technovations in Electrical Engineering & Green Energy System

Research Article (2022) 1(4):71-89

LRAPM: A Lightweight RFID Authentication Protocol for MIoT Systems

Alireza Abdellahi Khorasgani[1], *PhD Student*, Mahdi Sajadieh [1], *Assistant Professor*, Mohammad Rouhollah Yazdani [1], *Associate Professor*

[1] *Department of Electrical Engineering, Isfahan (Khorasgan) Branch, Islamic Azad University, Khorasgan, Isfahan, Iran*

Abstract:

In recent years, the Internet of Things (IoT) networks have extensively been used in various practical field, one of the most important of which is medical Internet of Things (MIoT). In these networks, radio frequency identification (RFID) is one of the main technologies in creating an authentication system that is able to efficiently identify and identify medical equipment and patients. Therefore, researchers in this field have proposed different authentication protocols for RFID-based MIOT systems and claimed that they are resistant to active and passive attacks. Contrary to their claims, most of these protocols are not resistant to conventional attacks. Fan et al. have recently proposed a lightweight RFID authentication scheme for cloud-based RFID health-care systems and claimed that it is sufficiently efficient and secure. In this paper , we analyzed the Fan et al protocole and demonstrated that their protocol is vulnerable to replay, reader impersonation, tag tracking, and de-synchronization attacks. Moreover, we show how the similarity of some of their protocol messages causes attack. Then, we propose an improved protocol (LRAMP) that is resistant to these and other known attacks in RFID authentication protocol. According to security analysis, we can see that the LRAPM protocol has a high level of security. This high security can only be achieved by adding a new message and changing other messages. A comparison of the performance of the LRAPM protocol shows that this protocol is comparable to similar protocols in terms of computational costs, storage costs and communication costs.

Keywords: MIOT, Lightweight authentication, Reader impersonation, De-synchronization.

Received: 24 August 2022
Revised: 02 October 2022
Accepted: 30 October 2022
Corresponding Author: Dr. Sayed Mahdi Sajadieh, m.sajadieh@khuisf.ac.ir
DOI: http://dx.doi.org/10.30486/teeges.2022.1968457.1039

فناوری‌های نوین در مهندسی برق و سیستم انرژی سبز

TEEGES

مقاله پژوهشی

LRAPM: پروتکل سبک‌وزن امنیتی RFID برای استفاده در سیستم‌های MIOT

علیرضا عبداللهی خوراسگانی[1]، *دانشجوی دکتری*، سیدمهدی سجادیه[1]، *استادیار* ، محمدروح اله یزدانی[1]، *دانشیار*

1- دانشکده مهندسی برق، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، خوراسگان، اصفهان، ایران

چکیده:

در سال‌های اخیر شبکه‌های اینترنت اشیاء (IOT) به صورت گسترده‌ای در حوزه‌های کاربردی مختلف بکار رفته‌اند. یکی از مهم‌ترین کاربردهای این فناوری، شبکه‌های اینترنت اشیاء پزشکی (MIOT) می‌باشد. در این شبکه‌ها، شناسایی به وسیله فرکانس‌های رادیویی (RFID) یکی از فناوری‌های اصلی در ایجاد سیستم احراز هویت است که قادر به تشخیص و شناسایی کارآمد تجهیزات پزشکی و بیماران است. برهمین‌اساس، محققان پروتکل‌های احراز هویت مختلفی را پیشنهاد داده‌اند که می‌توان از آن‌ها در سامانه‌های MIOT مبتنی بر RFID استفاده نمود. البته برخلاف ادعای طراحان مبنی بر امنیت بالای هریک از این پروتکل‌ها، اکثر آنها در برابر حملات مرسوم در این حوزه مقاوم نیستند. به‌تازگی فان و همکاران، یک طرح احراز هویت RFID سبک‌وزن برای سیستم‌های مراقبت بهداشتی RFID مبتنی بر ابر اطلاعات پیشنهاد کرده‌اند و ادعا می‌کنند که پروتکل آنها به اندازه کافی کارآمد است و امنیت بالایی را فراهم می‌کند. در این مقاله، نشان داده می‌شود که پروتکل آنها نسبت به حملات تکرار، جعل هویت برچسب‌خوان، ردیابی برچسب، ناهمزمان‌سازی آسیب‌پذیر است. علاوه‌براین، نشان داده می‌شود که چگونه شباهت برخی از پیام‌های پروتکل، باعث حمله می‌شود. سپس، پروتکل بهبودیافته (LRAMP) پیشنهاد می‌گردد که در برابر این حملات و سایر حملات شناخته شده مقاوم است. تحلیل‌های امنیتی، نشان می‌دهد که پروتکل LRAPMاز امنیت بالایی برخوردار است. این امنیت بالا تنها با افزودن یک پیام جدید و تغییر پیام‌های دیگر بدست می‌آید. مقایسه عملکرد پروتکل LRAPM نشان می‌دهد که این پروتکل از نظر هزینه‌های محاسباتی، هزینه‌های ذخیره‌سازی و هزینه‌های ارتباطی با پروتکل‌های مشابه قابل مقایسه است.

واژه های کلیدی: اینترنت اشیاء پزشکی، احراز هویت سبک‌وزن، جعل هویت برچسب‌خوان، ناهمزمان‌سازی

تاریخ دریافت: ۱۴۰۱/۰۶/۰۲

تاریخ بازنگری: ۱۴۰۱/۰۷/۱۰

تاریخ پذیرش: ۱۴۰۱/۰۸/۰۸

نویسنده‌ی مسئول: دکتر سید مهدی سجادیه، m.sajadieh@khuisf.ac.ir

DOI: http://dx.doi.org/10.30486/teeges.2022.1968457.1039

۱- مقدمه

امروزه شبکه‌های مبتنی بر اینترنت اشیاء IOT[۱] درصددند که ارتباط جامعی بین دستگاه‌های هوشمند ایجاد نمایند. این سامانه‌ها در حوزه‌هایی همچون مراقبت‌های سلامت، حمل و نقل، شبکه‌های هوشمند بکار گرفته شده‌است. با توجه به کاربرد بالای سامانه‌های اینترنت اشیاء در دستگاه‌های خدمات‌رسان بهداشتی/ درمانی، تعداد زیادی از شرکت‌ها سرمایه‌گذاری‌های عظیمی را در حوزه خدمات درمانی به عمل آورده‌اند. تمامی دستگاه‌های هوشمند به حسگرهایی برای تشخیص، دریافت و انتقال داده‌ها نسبت به محیط پیرامونی خود مجهز هستند. نظارت از راه دور بر سطح سلامت بیمار، مدیریت بلادرنگ بیماری[۲] از مزایای استفاده از حسگرها در دستگاه‌های پزشکی است. تحت چنین شرایطی هزینه‌های مراقبتی کاهش می‌یابند. علاوه بر این، کیفیت زندگی بیمار نیز ارتقا می‌یابد. از این‌رو سامانه‌های اینترنت اشیا در بخش مراقبتی و درمانی، به اینترنت اشیای پزشکی (MIOT[۳]) معروف هستند. در سامانه‌های MIOT امکان نگهداری و ذخیره داده‌های تعداد زیادی از بیماران و امکان تحلیل همیشگی اطلاعات ذخیره شده وجود دارد. این مسئله راندمان فعالیت‌های کاربردی در صنعت درمان/ مراقبت‌های بهداشتی ارتقا می‌دهد.[۱]

امروزه فناوری شناسایی امواج رادیویی RFID[۴] با امکان شناسایی از طریق سیگنال‌های امواج رادیویی برترین سامانه در حوزه اینترنت اشیاء پزشکی است [۲ و ۳]. یک سیستم RFID شامل سه مولفه برچسب، برچسب‌خوان و سرور است[۴]. در سیستم‌های پزشکی مبتنی بر RFID، برچسب روی بدن بیمار، انواع مختلف از دستگاه‌های پزشکی یا سیستم‌های انتقال دارو قرار می‌گیرد. برچسب‌خوان اطلاعات را از برچسب‌ها دریافت می‌کند و آن‌ها را برای انجام فعالیت‌های مدیریتی و سایر عملیات به سرورها انتقال می‌دهد. اطلاعات از سرورهای مختلف به سمت سرور ابری منتقل می‌شوند. این سرور ابری امکان دسترسی همیشگی به اطلاعات را برای پزشکان، بیماران و مدیریت بیمارستان فراهم می‌سازند. انتقال اطلاعات در سیستم RFID از طریق کانال‌های غیرایمن صورت می‌گیرد. بنابراین آن را در برابر تهدیدهای امنیتی مهم و جدی آسیب‌پذیر می‌سازد. از آنجایی که اطلاعات بیماران بشدت حساس هستند و زندگی بیمار به آن‌ها وابسته است، لذا دسترسی افراد غیرمجاز به این اطلاعات عواقب ناگواری را در پی دارد. پس به اعمال مکانیزم‌های امنیتی صحیح نیاز می‌باشد تا در حین تشخیص و انتقال داده‌ها، شرایط امنی را برای دستگاه‌های پزشکی هوشمند ایجاد شود. پس مهم‌ترین دغدغه در سیستم‌های MIOT احراز هویت موجودیت‌ها است.[۵]

با توجه به محدودیت منابع برچسب‌ها، استفاده از روش‌های رمزنگاری متقارن و کلید عمومی وجود ندارد. بنابراین در اکثر پروتکل‌های احراز هویت پیشنهادی از تکنیک‌های رمزنگاری سبک‌وزن همچون توابع hash سبک‌وزن[۶]، PRNG، و توابع منطقی (XOR و چرخش بیتی) استفاده می‌شود.[۷]

با توجه به آنچه گفته شد اساسی‌ترین مسئله در سامانه‌های RFID تامین امنیت و دستیابی به احراز هویت صحیح می‌باشد. در این راستا تلاش‌های فراوانی صورت گرفته و در نتیجه پروتکل‌های مختلفی بدین منظور برای این قبیل سامانه‌ها بوجود آمده است. لیکن اغلب این پروتکل‌ها دارای نقایص و ضعف‌هایی می‌باشند که موجب آسیب‌پذیری آن‌ها در برابر حملات گوناگون می‌شوند. به‌تازگی فان و همکارانش [۸] پروتکل احراز هویت جدیدی را برای سیستم‌های خدمات بهداشتی مبتنی بر محیط ابری پیشنهاد داده‌اند که به اعتقاد آن‌ها از سطح امنیتی بالایی برخوردار است. متاسفانه تحلیل امنیتی حاضر نشان می‌دهد که این پروتکل در برابر حمله جعل هویت برچسب‌خوان، ردیابی برچسب و ناهمزمان‌سازی برچسب و سرور آسیب‌پذیر است. در نهایت یک پروتکل احراز هویت جدید طراحی می‌گردد.

دستاوردهای مقاله

دستاوردهای پژوهش فعلی به شکل زیر قابل خلاصه سازی هستند :

- حفره‌های امنیتی پروتکل فان شناسایی و نشان داده‌شد علی رغم ادعای طراحان، پروتکل آن‌ها در برابر حمله تکرار ، جعل هویت برچسب‌خوان، ردیابی برچسب‌ها، حمله ناهمزمان‌سازی آسیب‌پذیر است.
- برای غلبه بر کمبودهای پروتکل فان و همکارانش، پروتکل احراز هویت سبک‌وزن LRAPM را ارائه می‌شود. در پروتکل LRAPM جهت ارتقاء سطح امنیتی، از انتقال پیام‌های مشابه در کانال‌های غیر ایمن پرهیز شده‌است. از طرفی، تولید عدد تصادفی توسط برچسب در پروتکل LRAPM باعث شد ایمنی این پروتکل ارتقاء یابد.
- امنیت پروتکل LRAPM از نظر کیفی مورد بررسی قرار داده می‌شود و سطح امنیتی پروتکل با سایر پروتکل‌های مشابه مقایسه می‌گردد.

- در نهایت نیز کارایی پروتکل LRAPM° طی جداول ۴ و ۵ با سایر پروتکل‌های مشابه مقایسه می‌شود.

ادامه این مقاله به صورت زیر سازمان‌دهی شده است: در بخش دوم بازبینی فعالیت‌های مربوطه و پروتکل‌های احراز هویت ارائه شده در چند سال گذشته در دستور کار قرار می‌گیرد. بخش سوم، به بازبینی پروتکل فان و همکارانش می‌پردازد. در بخش چهارم نقاط‌ضعف امنیتی پروتکل یادشده نمایان می‌شود. در بخش پنجم، پروتکل بهبود یافته‌ای برای غلبه بر این معایب امنیتی ارائه می‌گردد. بخش ششم نیز به تحلیل امنیت طرح مقاوم شده پیشنهادی پرداخته است. در نهایت نتایج مقاله در بخش هفتم بیان می‌گردد.

۲- کارهای مرتبط

در سال‌های اخیر پروتکل های احراز هویت RFID زیادی پیشنهاد شده‌اند. در تمامی آن‌ها سازگاری با سیستم‌های اینترنت اشیا مطرح شده است. این در حالیست که در بازه زمانی کوتاهی پس از معرفی آن‌ها، حفره‌های امنیتی در آن‌ها شناسایی و آشکار شده‌است.
چانگ یه و همکارانش در [۹] پروتکل احراز هویت RFID به نام SRP پیشنهاد کردند. آن‌ها از یک شاخص برای جست‌وجوی برچسب مورد نظر در پایگاه داده استفاده می‌کردند. حبیبی و همکارانش [۱۰] نشان دادند که پروتکل یه و همکارانش نیز قادر به فراهم کردن ارتباط امن نیست. آن‌ها بعد از آن ایجاد تغییراتی در آن پروتکل نسخه ارتقا یافته‌ای از آن را ارائه نمودند. محمدی و همکارانش در [۱۱] نشان دادند که پروتکل حبیبی و همکارانش در برابر حملات افشای پارامترهای مخفی، جعل هویت برچسب، ناهمزمان‌سازی و حمله ردیابی برچسب مقاوم نیست. آن‌ها یک پروتکل احراز هویت فوق‌سبک‌وزن با نام ILMAP ارائه کردند. علوی و همکارانش در [۱۲] نشان دادند که پروتکلILMAP ، نسبت به حملات ردیابی و افشای برخی پارامترهای مخفی آسیب‌پذیر است و نمی‌تواند امنیت روبه‌جلو را به خوبی حفظ کند. کابایرو ژیل و همکاران [۱۳] پروتکل احراز هویت با استفاده از یک تابع مولد اعداد شبه تصادفی PRNG پیشنهاد دادند اما در [۱۴] مرادی و همکاران نشان دادند پروتکل قبلی در برابر حملات ردیابی برچسب، جعل هویت برچسب و ناهمزمانی مقاوم نیست. تئواری و گوپتا [۱۵] یک پروتکل احراز هویت RFID را پیشنهاد دادند که برای محیط‌های IOT کاربرد دارد . آن‌ها مدعی شدند که پروتکل پیشنهادی در برابر حملات ناهمزمان‌سازی، افشای پارامترهای مخفی و ردیابی مقاوم است. در سال‌های بعد، محققان در مراجع [۱۶ و ۱۷] آسیب‌پذیری این پروتکل در برابر حملات افشای پارامترهای مخفی را به اثبات رساندند. فان و همکاران [۱۸] پروتکلی با عنوان LRMAPC را برای سامانه‌های اینترنت اشیاء معرفی کردند. آن‌ها ادعا کردند که پروتکلشان از امنیت بالاتری نسبت به سایر پروتکل‌های موجود برخوردارست. با این‌وجود، محققان در [۱۹] نشان دادند که پروتکل LRMAPC در برابر حملات جعل هویت برچسب-خوان آسیب‌پذیرست.
سریواستاوا و همکاران در [۲۰]، پروتکل امنی را بر اساس تابع hash و کلید رمز اشتراکی بین برچسب و سرور معرفی کردند. از این روش تحت عنوان سیستم اطلاعات پزشکی- مراقبت از راه دور (TMIS) یاد می‌شود. لی و همکاران در [۲۱] متوجه شدند که پروتکل معرفی شده [۲۰] در برابر حملات مختلفی همچون خنثی‌سازی احراز هویت دوطرفه آسیب‌پذیرست و فاقد مقیاس‌پذیری می‌باشد. آنها در [۲۱۰] پروتکل یادشده را بهبود بخشیدند. قائم‌مقامی و همکاران در [۲۲] نشان دادند روش پیشنهادی [۲۱] در برابر حملاتی همچون ناهمزمان‌سازی و جعل برچسب‌خوان آسیب پذیرست.
هی و همکارانش در [۲۳] یک پروتکل احراز هویت سبک‌وزن مبتنی بر ECC را برای سیستم‌های RFID پیشنهاد دادند. این پروتکل برای کاربردهای درمانی- بهداشتی موبایلی پیشنهاد شده‌است. اما لی و همکارانش در [۲۴] نشان داده‌اند که پروتکل پیشنهادی [۲۳] در برابر حمله ردیابی آسیب‌پذیر است. در ادامه کار، محققان روش‌های دیگری همچون روش مبتنی بر شبکه پتری [۲۵] و روش پیش محاسباتی در برچسب برای تأمین امنیت مبتنی بر ECC [۲۶] پیشنهاد دادند.
وُو و همکاران در [۲۷]، پروتکل احراز هویت سبک‌وزن و مبتنی بر hash برای RFIDها معرفی کردند. پروتکل پیشنهادی برای سیستم‌های درمانی از سیستم دستیار ابری استفاده می‌کند. محققان این پروتکل اثبات کردند که پروتکلشان گمنامی لازم را نسبت به برچسب و برچسب‌خوان فراهم می‌سازد و از نظر امنیت روبه‌جلو و روبه‌عقب غیرقابل ردیابی می‌باشد. بن‌صالح و همکارانش در [۲۷] یک پروتکل احراز هویت، براساس امضای خم بیضوی پیشنهاد دادند. این پروتکل قادر به تضمین امنیت اسناد پزشکی بیماران و کادر درمانی می‌باشد. بازیابی پیام نیز در این پروتکل لحاظ شده است.

به‌تازگی فان و همکارانش در [۸] یک پروتکل احراز هویت دو طرفه سبک‌وزن معرفی کردند. محققان این پروتکل مدعی شدند که روش پیشنهادی از ویژگی‌های امنیتی مناسب و مورد نیاز سیستم‌های RFID برخوردارست و مناسب سیستم‌های خدمات بهداشتی مبتنی بر اینترنت اشیاء می‌باشد. در این مقاله نشان داده می‌شود که پروتکل پیشنهادی فان و همکارانش دارای آسیب‌های امنیتی جدی همچون تکرار و جعل هویت برچسب‌خوان، ردیابی برچسب و ناهمزمان‌سازی است.

۳- مروری بر پروتکل فان و همکارانش

در سال ۲۰۱۹ فان و همکاران یک پروتکل احراز هویت RFID سبک‌وزن به منظور غلبه بر مشکلات امنیتی و حریم خصوصی سیستم‌های خدمات بهداشتی مبتنی بر محیط ابری را معرفی کردند و چنین ادعا کردند که این پروتکل از کارایی بسیار بالایی برخوردارست. فرض بر این است که چنین پروتکلی قادر به مقاومت در برابر حملات وارده به RFID از جمله جعل هویت برچسب‌خوان، ردیابی برچسب و ناهمزمان‌سازی است[۸]. آن‌ها تلاش نمودند با استفاده از به‌کارگیری عملیات‌های سبک‌وزن و ساده در سمت برچسب تعادل خوبی بین هزینه‌ها و سطح امنیت موجود فراهم نمایند. آنها با استفاده از تمبرهای زمانی به دنبال خنثی‌سازی حملات جعل هویت بودند. از طرفی دیگر ادعای آن‌ها این است که ذخیره کلیدهای قدیمی در سرور، باعث مقاومت در برابر حمله ناهمزمان‌سازی می‌شود . توصیف این پروتکل در ادامه کار ارائه شده است.

۳-۱- علایم اختصاری

علایم اختصاری در طول این مقاله در جدول ۱ نمایش داده شده‌است. در مقاله حاضر از عملیات‌های ساده‌ای همچون XOR، مولد اعداد شبه تصادفیPRNG، شیفت چرخشی Rot(x,y)، جمع استفاده می‌شود.

جدول (۱) علایم اختصاری

توضیحات	علامت اختصاری
دو عدد اول بزرگ	p,q
n=pq.	N
شبه شناسه برچسب که از روی شناسه اصلی ساخته شده است	SID
شبه شناسه قبلی برچسب در سروری ابری	SID_{old}
شبه شناسه برچسب‌خوان	SRID
شبه شناسه قبلی برچسب‌خوان در سرور ابری	$SRID_{old}$
کلید ذخیره شده در برچسب	X
$X^2 mod n$, n=pq	X′
کلید ذخیره شده در برچسب‌خوان	Y
$Y^2 mod n$, n=pq	Y′
زمان فعلی X	T_X
مقدار آستانه زمانی	T_{th}
عملیات XORبیتی	$\oplus$
مولد اعداد شبه تصادفی	PRNG()
انتقال به چپ X⊕Y به اندازه y mod L بیت ، L نشان دهنده طول y است. مثال : X=10110101 , Y=10101000 , Rot(X,Y)=11101000	Rot (X,Y)

۳-۲- روش پیشنهادی فان و همکاران

نمایی از روش پیشنهادی فان و همکارانش در شکل ۱ به نمایش درآمده است. این روش شامل یک مرحله راه‌اندازی، یک مرحله احراز هویت و یک مرحله به‌روزرسانی است. در مرحله راه‌اندازی، مدیر سیستم مقادیر اولیه‌ای را به تمامی اعضای سیستم تخصیص می‌دهد. احراز هویت دوطرفه در مرحله احراز هویت صورت می‌گیرد. کلیدهای مخفی در مرحله به‌روزرسانی تحت به‌روزرسانی قرار می‌گیرند.

مرحله راه‌اندازی: در این مرحله، برخی مولفه‌های معتبر موجود در سیستم به شرح زیر تعریف می‌شوند:

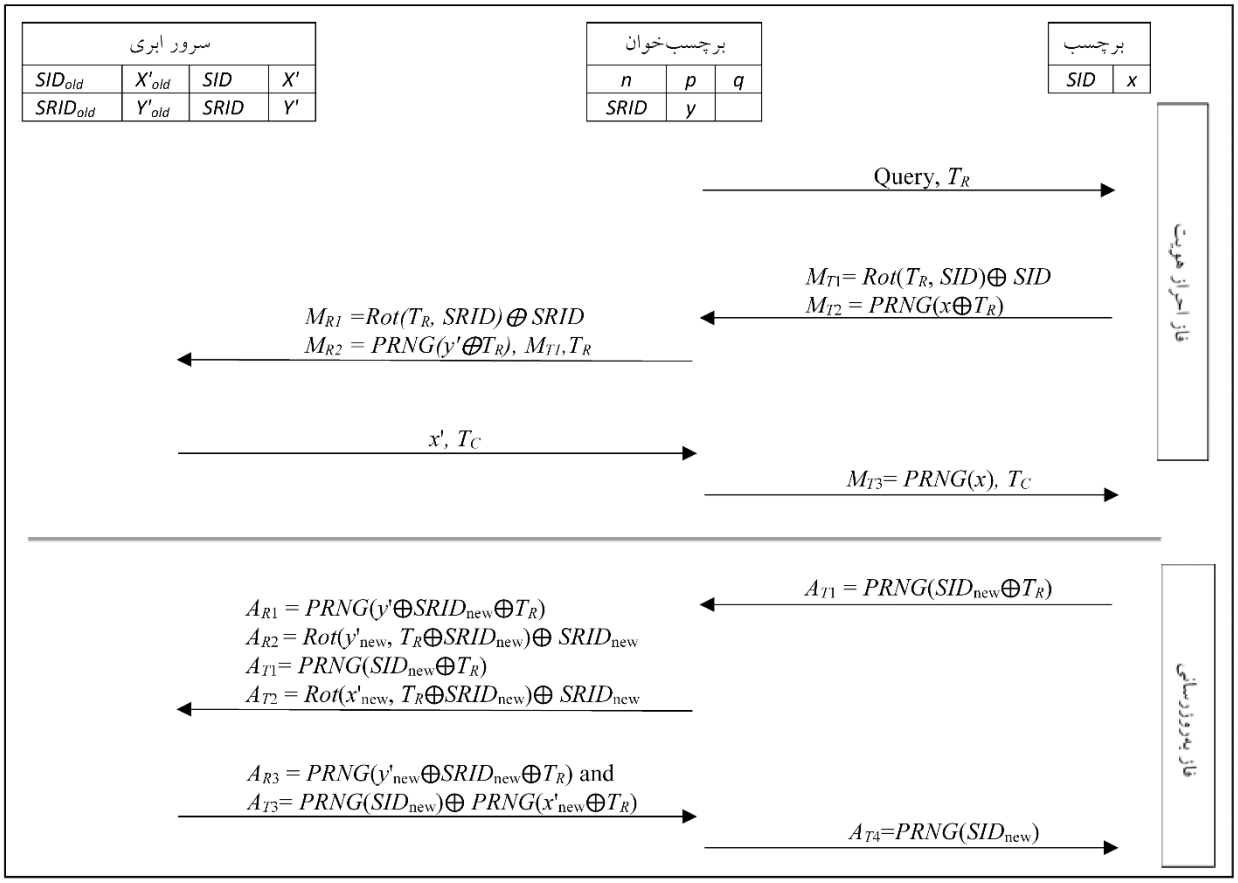
الف – ابتدا دو عدد اول بزرگ p و q (۵۱۲ بیت یا بیشتر پیشنهاد می‌شود) تولید و مقدار n=pq محاسبه می‌گردد. سپس هر سه مقدار n، p و q برروی هر برچسب‌خوان مجاز ذخیره می‌شود.

ب- مدیر سیستم یک شبه شناسه (SID) و یک کلید مخفی (x) را به هر برچسب معتبر تخصیص می‌دهد.

پ- مدیر سیستم یک شبه شناسه (SRID) و یک کلید مخفی (y) را به هر برچسب‌خوان معتبر تخصیص می‌دهد

ت- مدیر سیستم برای هر برچسب معتبر، مقادیر SID=SID و $x'=x^2 modn$ در جدول داده‌های شاخص برچسب که در سرور ابری ذخیره شده‌است قرار می‌دهد. در این مرحله به صورت پیش فرض SID_{old} و x'_{old} هر دو برابر با صفر قرار می‌گیرند.

ث- مدیر سیستم برای هر برچسب‌خوان معتبر، مقادیر SRID=SRID و $y'=y^2 modn$ در جدول داده‌های شاخص برچسب‌خوان که در سرور ابری ذخیره شده‌است قرار می‌دهد. در این مرحله به صورت پیش‌فرض $SRID_{old}$ و y'_{old} هر دو برابر با صفر قرار می‌گیرند.



شکل (۱): پروتکل احراز هویت فان و همکاران

مرحله احراز هویت :

الف) برچسب‌خوان به برچسب: برچسب‌خوان کوئری و زمان فعلی T_R را برای برچسب ارسال می‌کند.

ب) برچسب به برچسب‌خوان: برچسب مقادیر M_{T1} و M_{T2} را بر اساس T_R، SID و x طبق روابط (۱) و (۲) محاسبه و جهت احراز هویت برای برچسب‌خوان ارسال می‌کند.

$$M_{T1}= Rot(T_R, SID) \oplus SID \quad (۱)$$

$$M_{T2} = PRNG(x \oplus T_R) \quad (۲)$$

پ) برچسب‌خوان به سرور ابری: برچسب‌خوان پس از دریافت پیام M_{T1} و M_{T2} مقادیر M_{R1} و M_{R2} را طبق روابط (۳) و (۴) محاسبه و جهت احراز هویت پیام $\{M_{R1}, M_{R2}, M_{T1}, T_R\}$ را برای سرور ابری ارسال می‌نماید.

$$M_{R1} =Rot(T_R, SRID) \oplus SRID \quad (۳)$$

$$M_{R2} = PRNG(y' \oplus T_R) \quad (۴)$$

ت) سرور ابری به برچسب‌خوان: پس از دریافت پیام از طرف برچسب‌خوان، سرور ابری در ابتدا وجود رابطه $T_{th1} < T_S - T_R < T_{th2}$ بررسی می‌کند. در صورت برقراری این شرایط، سرور ابری مقدار SRID را از جدول داده‌های شاخص برچسب‌خوان جستجو کرده تا مقدار

تطبیقی برای M_{R1} یافت شود. در صورت وجود تطابق، سرور ابری مقدار 'y متناظر را استخراج کرده و M_{R2}' را طبق رابطه (۴) محاسبه می‌کند. در صورتی که $M_{R2}'=M_{R2}$ باشد، سرور ابری اعتبار برچسب‌خوان را تایید می‌کند. در ادامه سرور مقدار SID در جدول داده‌های شاخص برچسب جستجو می‌کند تا مقدار تطبیقی برای M_{T1} بیابد. در صورت وجود تطبیق، سرور ابری 'x مربوطه را بازیابی و به همراه زمان فعلی (T_C) به سمت برچسب‌خوان می‌فرستد.

ث) برچسب‌خوان به برچسب: برچسب‌خوان چهار راه‌حل x_1، x_2، x_3 و x_4 را بر اساس 'x ، p، q بدست می‌آورد. سپس براساس این راه‌حل مقدار M_{T2}' را طبق رابطه (۲) محاسبه تا برابری $M_{T2}'= M_{T2}$ حاصل و مقدار $x=x_i$ صحیح بدست آید. در چنین شرایطی برچسب احراز هویت شده‌است، برچسب‌خوان مقدار M_{T3} را طبق رابطه (۵) محاسبه کرده و پیام $\{M_{T3}, T_C\}$ را برای برچسب می‌فرستد.

$$M_{T3} = PRNG(x) \quad (۵)$$

پس از دریافت پیام $\{M_{T3}, T_C\}$ توسط برچسب، ابتدا اعتبار برچسب‌خوان با بررسی $M_{T3}= PRNG(x)$ تعیین می‌شود. در صورت برقراری این وضعیت، هویت برچسب‌خوان به عنوان برچسب‌خوان مجاز به اثبات می‌رسد. در حقیقت صرفاً برچسب‌خوان مجاز با برخورداری از مقادیر p و q قادر به یافتن x از روی 'x است. در این شرایط احراز هویت دو طرفه انجام شده‌است و مرحله به‌روزرسانی آغاز می‌شود.

مرحله به‌روزرسانی

ج) برچسب به برچسب‌خوان: برچسب با استفاده از روابط (۶) و (۷)، مقادیر SID_{new} و x_{new} رامحاسبه می‌کند. سپس مقدار A_{T1} را طبق رابطه (۸) محاسبه و به سمت برچسب‌خوان انتقال می‌دهد تا اطلاع‌رسانی به‌روزرسانی به سرور ابری ارسال شود.

$$SID_{new} = SID + T_C \quad (۶)$$

$$x_{new} = Rot(x, T_C) \oplus T_C \quad (۷)$$

$$A_{T1} = PRNG(SID_{new} \oplus T_R) \quad (۸)$$

چ) برچسب‌خوان به سرور ابری: پس از دریافت A_{T1}، به منظور به‌روزرسانی داده‌های برچسب در سرور ابری، برچسب‌خوان مقدار x_{new} را ازطریق رابطه (۷) محاسبه و x'_{new} را طبق رابطه (۹) محاسبه می‌کند. علاوه بر این مقادیر $SRID_{new}$، y_{new} و y'_{new} طبق روابط (۱۰) الی (۱۲) محاسبه شده تا داده‌های برچسب‌خوان نیز در سرور ابری به‌روزرسانی شوند.

$$x'_{new} = x^2_{new} \bmod n \quad (۹)$$

$$SRID_{new} = SRID + T_C \quad (۱۰)$$

$$y_{new} = Rot(T_C, y) \quad (۱۱)$$

$$y'_{new} = y^2_{new} \bmod n \quad (۱۲)$$

در ادامه برچسب‌خوان مقادیر جدید را به صورت مخفی از طریق A_{R1}، A_{R2} ، A_{T1} و A_{T2} که طبق روابط (۱۳) الی (۱۶) محاسبه می‌شوند، برای سرور ابری ارسال می‌نماید.

$$A_{R1} = PRNG(y' \oplus SRID_{new} \oplus T_R) \quad (۱۳)$$

$$A_{R2} = Rot(y'_{new}, T_R \oplus SRID_{new}) \oplus SRID_{new} \quad (۱۴)$$

$$A_{T1} = PRNG(SID_{new} \oplus T_R) \quad (۱۵)$$

$$A_{T2} = Rot(x'_{new}, T_R \oplus SRID_{new}) \oplus SRID_{new} \quad (۱۶)$$

ح) سرور ابری به برچسب‌خوان: پس از اینکه سرور ابری پیام $\{A_{R1}, A_{R2}, A_{T1}, A_{T2}\}$ را دریافت می‌کند، مقدار $SRID_{new}$ را به عنوان اولین گام محاسبه می‌کند. سپس سرور ابری A_{R1} را محاسبه و بررسی می‌کند که آیا با A_{R1} ارسالی برابر است یا خیر. در صورت برقراری این شرایط، سرور ابری مقدار y'_{new} را از A_{R2} بدست می‌آورد و شروع به به‌روزرسانی جدول داده‌های شاخص برچسب‌خوان به کمک مقادیر جدید می‌نماید. در صورتی‌که مقادیر SRID و 'y از طریق داده‌های قدیمی جدول قابل دسترسی باشند، سرور ابری مقادیر $SRID_{new}$ و y'_{new} را به‌صورت $SRID_{new} \rightarrow SRID$ و $y'_{new} \rightarrow y'$ به‌روز می‌کند. در اینجا مقادیر $SRID_{old}$ و y'_{old} به همان صورت قبل باقی می‌مانند. در صورت مشاهده SRID و 'y در داده‌های جدید، سرور ابری مقادیر را به‌صورت $SRID \rightarrow SRID_{old}$ ، $y' \rightarrow y'_{old}$، $SRID_{new} \rightarrow SRID$ ، $y'_{new} \rightarrow y'$ به‌روز می‌کند. به طریق مشابه، سرور ابری مقدار SID_{new} را محاسبه کرده و سپس صحت A_{T1} ارسالی را

بررسی می‌کند. در صورت درستی A_{T1}، سرور ابری مقدار X'_{new} را از A_{T2} استخراج کرده و جدول داده‌های شاخص برچسب را با مقادیر جدید به‌روزرسانی می‌کند. در صورت یافتن SID و x' در بخش داده‌های قدیمی، سرور ابری مقادیر SID_{new} و x'_{new} را به‌صورت $SID_{new} \rightarrow SID$ و $x'_{new} \rightarrow x'$ به‌روز می‌کند. در اینجا مقادیر SID_{old} و x'_{old} به همان صورت قبل باقی می‌مانند. در صورت مشاهده SID و x' در داده‌های جدید، سرور ابری مقادیر را به‌صورت $SID \rightarrow SID_{old}$ ، $x' \rightarrow x'_{old}$ ، $SID_{new} \rightarrow SID$ ، $x'_{new} \rightarrow x'$ به‌روز می‌کند. در نهایت سرور ابری مقادیر A_{R3} و A_{T3} را طبق روابط (۱۷) و (۱۸) محاسبه و به عنوان پاسخ برچسب‌خوان و برچسب برای برچسب‌خوان ارسال می‌نماید.

$$A_{R3} = PRNG(y'_{new} \oplus SRID_{new} \oplus T_R) \quad (۱۷)$$

$$A_{T3} = PRNG(SID_{new}) \oplus PRNG(x'_{new} \oplus T_R) \quad (۱۸)$$

خ) برچسب‌خوان به برچسب: پس از دریافت A_{T3} و A_{R3}، برچسب‌خوان بررسی صحت A_{R3} ارسالی از طرف سرور ابری را بررسی و در صورت درستی و اصالت آن، بدین نتیجه می‌رسد که سرور ابری جدول داده‌های شاخص برچسب‌خوان را با موفقیت به‌روزرسانی کرده است. در ادامه برچسب‌خوان مقادیر $SRID_{new}$ و y_{new} را با SRID و y جایگزین می‌کند. علاوه بر این، برچسب‌خوان مقدار A_{T4} را طبق رابطه (۱۹) محاسبه و آن را برای برچسب می‌فرستد.

$$A_{T4} = A_{T3} \oplus PRNG(x'_{new} \oplus T_R) \quad (۱۹)$$

پس از دریافت A_{T4}، برچسب صحت درستی A_{T4} را بررسی و در صورت تأیید آن، متوجه می‌شود سرور ابری با موفقیت جدول داده‌های شاخص برچسب را به‌روزرسانی کرده‌است. سپس برچسب مقادیر SID_{new} و x_{new} را جایگزین SID و X می‌کند.

۴- تحلیل امنیتی پروتکل فان و همکارانش

در این قسمت نشان داده می‌شود که پروتکل فان و همکارانش چگونه در برابر حملات ردیابی برچسب، تکرار و جعل هویت برچسب‌خوان و حمله ناهمزمان سازی آسیب پذیر است. در این پروتکل برچسب هیچ عدد تصادفی یا تمبر زمانی ایجاد نمی‌کند. از طرفی دیگر برچسب در مرحله احراز هویت تمبر زمانی ارسالی از طرف برچسب‌خوان را از لحاظ صحت بررسی نمی‌کند از این‌رو این تمبر زمانی از دید برچسب مانند یک nonce به نظر می‌آید. همچنین در مرحله احراز هویت و مرحله به‌روزرسانی از پیام‌هایی تقریبا مشابه به هم استفاده شده‌است. مهاجم نیز از این ویژگی ها استفاده می‌کند و حملات یاد شده را تحقق می‌بخشد.

۴-۱- حمله ردیابی برچسب

در این نوع حمله مهاجم سعی می‌کند یک برچسب هدف را مورد ردیابی قرار دهد. این حمله نیز شامل ۳ مرحله است :

مرحله ۱ : در این مرحله از حمله مهاجم پیام‌های رد و بدل شده بین برچسب و برچسب‌خوان و سرور را در یک دور اجرای پروتکل مورد استراق سمع قرار می‌دهد. مهاجم مقادیر T_R ، $M_{T1}=Rot(T_R, SID) \oplus SID$ و $M_{T2}=PRNG(x \oplus T_R)$ را ذخیره می‌کند و در انتها از رسیدن پیام $A_{T4} = PRNG(SID_{new})$ از برچسب‌خوان به برچسب جلوگیری می‌کند. بنابراین برچسب مقادیر x و SID را به روزرسانی نمی‌کند و همان مقادیر قبلی باقی می‌ماند.

مرحله ۲ : در این مرحله مهاجم در نقش برچسب‌خوان، یک جلسه را آغاز می‌کند و مقدار T_R را به برچسب ارسال می‌کند. طبق روند پروتکل برچسب به محض دریافت T_R مقادیر $M_{T1}'=Rot(T_R, SID_2) \oplus SID_2$ و $M_{T2}'=PRNG(X_2 \oplus T_R)$ محاسبه می‌کند. سپس برچسب مقادیر M_{T1}' و M_{T2}' را برای مهاجم ارسال می‌کند.

مرحله ۳ : با توجه به اینکه مهاجم در مرحله اول از به‌روزرسانی مقادیر x و SID در سمت برچسب جلوگیری کرد، پس پیام‌های M_{T1}' و M_{T2}' که توسط برچسب هدف تولید می‌شود همان مقادیر M_{T1} و M_{T2} است که در مرحله اول استراق سمع شده‌است. اکنون در صورتی که شرط $M_{T1}'=M_{T1}$ و $M_{T2}'=M_{T2}$ برآورده شده‌باشد، آنگاه نتیجه‌گیری این است که برچسبِ مرحله استراق‌سمع، با برچسبِ هدفِ مهاجم تطابق دارد. در این صورت مهاجم می‌تواند برچسب هدف را از بین دیگر برچسب‌ها تشخیص دهد و ردیابی نماید.

۴-۲- حمله تکرار و جعل هویت برچسب‌خوان

در حمله جعل هویت برچسب‌خوان مهاجم تلاش می‌کند تا ضمن فریب دادن برچسب خود را به عنوان یک برچسب‌خوان معتبر برای برچسب معرفی کند. این حمله شامل ۲ مرحله است : ۱- مرحله یادگیری، ۲- مرحله اجرا که در ادامه توصیف می‌شوند.

۱- مرحله یادگیری : در این مرحله مهاجم اطلاعات مربوطه را از طریق استراق‌سمع، تنها در یک دور از اجرای پروتکل بدست می‌آورد و از به‌روزرسانی پارامترهای مخفی برچسب جلوگیری می‌کند. روال عملیات این مرحله بدین نحو است:

- ✓ مهاجم یک اجرای کامل پروتکل را مورد استراق‌سمع قرار می‌دهد.
- ✓ مهاجم پیام های T_R ، $M_{T1}=Rot(T_R ,SID)\oplus SID$ ، $M_{T2}=PRNG(x\oplus T_R)$ ، T_c ، $M_{T3}=PRNG(x)$ و $A_{T4}=PRNG(SID_{new})$ را ذخیره می‌کند.
- ✓ مهاجم از رسیدن پیام $A_{T4} =PRNG (SID_{new})$ از برچسب‌خوان به برچسب جلوگیری می‌کند. بنابراین برچسب مقادیر x و SID را به روزرسانی نمی‌کند و همان مقادیر قبلی باقی می‌ماند.

۲- مرحله اجرای حمله: در این مرحله مهاجم با استفاده از اطلاعات ذخیره شده در مرحله یادگیری حمله را به صورت زیر اجرا می‌کند

- ✓ مهاجم در نقش برچسب‌خوان عمل می‌کند و مقدار T_R را برای برچسب ارسال می‌کند.
- ✓ برچسب پس از دریافت T_R، پیام‌های $M_{T1}=Rot(T_R ,SID)\oplus SID$ ، $M_{T2}=PRNG(X\oplus T_R)$ را تولید می‌کند سپس برچسب مقادیر M_{T1} و M_{T2} را برای مهاجم ارسال می‌کند.
- ✓ به محض دریافت M_{T1} و M_{T2} ، مهاجم که در نقش برچسب‌خوان جعلی است پیام T_c ، $M_{T3}=PRNG(x)$ که در مرحله یادگیری استراق‌سمع کرده برای برچسب ارسال می‌کند.
- ✓ به محض دریافت T_c ، $M_{T3}=PRNG(x)$ ، برچسب از T_c استفاده کرده و مقادیر SID_{new} و X_{new} را محاسبه می‌کند. سپس مقدار $A_{T1}= PRNG (SID_{new}\oplus T_R)$ را به مهاجم انتقال می‌دهد.
- ✓ با دریافت A_{T1}، این بار مهاجم $A_{T4} =PRNG (SID_{new})$ را به برچسب ارسال می‌کند.
- ✓ به محض دریافت A_{T4}، برچسب مقدار A_{T4} دریافتی را با مقدار $PRNG(SID_{new})$ مقایسه می‌کند. با توجه به اینکه مهاجم در مرحله یادگیری از به‌روزرسانی پارامترهای مخفی برچسب جلوگیری نمود و در مرحله قبل نیز T_c استراق‌سمع شده از قبل را برای برچسب ارسال نمود پس $A_{T4} =PRNG (SID_{new})$ خواهد بود و برچسب مهاجم را به عنوان برچسب‌خوان قانونی مورد تایید قرار می‌دهد.

بدین‌ترتیب با انجام این حمله، هویت برچسب‌خوان توسط عامل مهاجم جعل می‌شود. احتمال موفقیت این حمله "۱" است، در حالی‌که پیچیدگی آن تنها در حد یک نشست استراق سمع، قطع یک پیام و ارسال مجدد پیام‌ها است. در حقیقت این حمله توسط هر مهاجمی با قابلیت استراق سمع قابل اجراست. بنابراین مهاجم از نوع غیرفعال در نظر گرفته می‌شود.

۴-۳- حمله ناهمزمان سازی

در این نوع حمله مهاجم کاری می‌کند تا پارامترهای مخفی مشترک بین برچسب و سرور در مرحله به‌روزرسانی طوری تغییر کنند که طرف مقابل از این نوع به‌روزرسانی آگاهی نداشته باشد. در این‌صورت موارد مخفی برچسب و سرور اشتراکی ندارند. از این به بعد برچسب نمی‌تواند با برچسب‌خوان و سرور ارتباط داشته‌باشد. این حمله شامل ۵ مرحله است.

مرحله ۱: در این مرحله مهاجم در نقش برچسب‌خوان مقدار $T_R=0$ را برای برچسب ارسال می‌کند.

مرحله ۲: از آنجایی که تمبر زمانی T_R برای برچسب مثل یک Nonc می‌ماند به محض دریافت T_R، پیام‌های $M_{T1}=Rot(0 ,SID)\oplus SID$ ، $M_{T2}=PRNG(x\oplus 0)=PRNG(x)$ را محاسبه کرده و برای مهاجم ارسال می‌کند.

مرحله۳: در این مرحله مهاجم جهت اثبات خود برای برچسب نیاز به پیام $M_{T3}=PRNG(x)$ دارد. این مقدار در مرحله قبل توسط برچسب برای مهاجم ارسال شده‌است پس مهاجم در نقش یک برچسب‌خوان عمل کرده و مقادیر T_A و $PRNG(x)$ را به سمت برچسب می‌فرستد.

مرحله ۴: حال برچسب هویت مهاجم را تایید کرده مقادیر $SID_{NEW}=SID+T_A$ و $X_{NEW}= rot(x,T_A) \oplus T_A$ را محاسبه می‌کند. سپس مقدار $A_{T1}= PRNG(SID_{new} \oplus 0)= PRNG(SID_{new})$ را به برچسب‌خوان انتقال می‌دهد.

مرحله ۵: در این مرحله مهاجم نیاز به پیام $A_{T4}=PRNG(SID_{new})$ دارد. این مقدار در مرحله قبل توسط برچسب برای مهاجم ارسال شده است پس مهاجم در نقش یک برچسب‌خوان عمل کرده و مقدار $PRNG(SID_{new})$ را به برچسب می‌فرستد.

مرحله ۶: حال برچسب هویت مهاجم را تایید می‌کند. سپس برچسب مقادیر SID_{new} و x_{new} را جایگزین SID و x می‌کند. این در حالی است که سرور از این به‌روزرسانی آگاهی ندارد. بنابراین حمله ناهمزمان‌سازی با موفقیت صورت می‌گیرد.

با انجام این حمله، مهاجم توانست اشتراک بین پارامترهای مخفی برچسب و سرور را از بین ببرد. در حالی‌که پیچیدگی آن تنها در حد ارسال و دریافت چند پیام می‌باشد. در حقیقت این حمله توسط هر مهاجمی با قابلیت ارسال و دریافت پیام قابل اجراست.

۵- پروتکل اصلاح شده LRAPM

در ادامه مقاله پروتکل احراز هویت سبک‌وزن LRAPM پیشنهاد می‌گردد تا خلاءهای امنیتی پروتکل فان و همکاران برطرف شود. این پروتکل امنیت بالاتری از پروتکل قبلی به ارمغان می‌آورد.

در پروتکل پیشنهادی به منظور غلبه بر حملات معرفی شده برچسب یک عدد تصادفی جدید تولید می‌کند. برچسب از این عدد تصادفی در پیام‌ها استفاده کرده تا از دریافت و تایید پیام‌های قدیمی جلوگیری کند. از طرفی در پایان هر نشست تمبر زمانی T_C با نام T_T در برچسب ذخیره می‌شود بنابراین در شروع جلسه بعد، برچسب T_R که از طرف برچسب‌خوان ارسال شده است را با T_T مقایسه می‌کند و اگر T_R بزرگتر از T_T بود به اجرای پروتکل ادامه می‌دهد. در این صورت مهاجم نمی‌تواند پیام‌های نشست‌های قبلی به برچسب را ارسال نماید. یکی دیگر از ویژگی‌های این پروتکل آن است که به جای استفاده مستقیم از شناسه برچسب ID از شبه‌شناسه برچسب SID و به جای RID از شبه‌شناسه SRID برای برچسب‌خوان استفاده شده است. در این‌صورت پس از هربار اجرای موفق پروتکل شبه‌شناسه‌ها به‌روز می‌شوند و در جلسات بعدی از آن‌ها برای اجرای پروتکل استفاده می‌گردد و از شناسه ثابت استفاده نمی‌گردد بنابراین از بروز حملاتی هم‌چون تکرار و ردیابی جلوگیری می‌شود. علاوه بر این ادعا می‌شود که پروتکل پیشنهادی در برابر تمامی حملات متداول در اینترنت اشیای مبتنی بر RFID مقاوم است. پروتکل LRAPM شامل سه مرحله راه‌اندازی، احراز هویت و به‌روزرسانی می‌باشد. نمایی از پروتکل پیشنهادی در شکل (۲) ترسیم شده است.

مرحله راه‌اندازی : این مرحله از پروتکل پیشنهادی همانند پروتکل فان و همکارانش بوده و به شرح زیر تعریف می‌شود:

الف – ابتدا دو عدد اول بزرگ p و q (۵۱۲ بیت یا بیشتر پیشنهاد می‌شود) تولید و مقدار n=pq محاسبه می‌گردد. سپس هر سه مقدار n، p و q برروی هر برچسب‌خوان مجاز ذخیره می‌شود.

ب- مدیر سیستم یک شبه شناسه (SID) و یک کلید مخفی (x) را به هر برچسب معتبر تخصیص می‌دهد.

پ- مدیر سیستم یک شبه شناسه (SRID) و یک کلید مخفی (y) را به هر برچسب‌خوان معتبر تخصیص می‌دهد

ت- مدیر سیستم برای هر برچسب معتبر، مقادیر SID=SID و $x'=x^2 \bmod n$ در جدول داده‌های شاخص برچسب که در سرور ابری ذخیره شده‌است قرار می‌دهد. در این مرحله به صورت پیش فرض SID_{old} و x'_{old} هر دو برابر با صفر قرار می‌گیرند.

ث- مدیر سیستم برای هر برچسب‌خوان معتبر، مقادیر SRID=SRID و $y'=y^2 \bmod n$ در جدول داده‌های شاخص برچسب‌خوان که در سرور ابری ذخیره شده‌است قرار می‌دهد. در این مرحله به صورت پیش فرض $SRID_{old}$ و y'_{old} هر دو برابر با صفر قرار می‌گیرند.

ث- برای هر برچسب‌خوان معتبر، مدیر سیستم SRID=SRID و $y'=y^2 \bmod n$ را از روی جدول داده شاخص شده برچسب‌خوان، ذخیره شده در سرور ابری تعریف می‌کند. $SRID_{old}$ و Y'_{old} هر دو برابر با صفر قرار می‌گیرند.

مرحله احراز هویت :

الف) برچسب‌خوان به برچسب : برچسب‌خوان یک برچسب زمان فعلی (T_R) را تولید می‌کند که بزرگتر از T_T است. این مقدار همراه با درخواست به برچسب ارسال می‌شود.

ب) برچسب به برچسب‌خوان : به محض دریافت درخواست، برچسب برقراری شرط $T_R>T_T$ را بررسی می‌کند. در صورتی که این شرط برقرار نباشد، برچسب ارتباط را قطع می‌کند. در غیر اینصورت عدد تصادفی R_T را ایجاد می‌کند. سپس برچسب مقادیر M_{T1}، M_{T2} وM_{T3} را طبق روابط (۲۰) الی (۲۲) محاسبه می‌کند. در ادامه برچسب مقدار چندتایی M_{T1},M_{T2},M_{T3} را به برچسب‌خوان ارسال می‌کند.

$$M_{T1}=R_T \oplus SID \quad (۲۰)$$

$$M_{T2}=Rot\ (T_R\ ,SID+R_T)\oplus SID \quad (۲۱)$$

$$M_{T3}=PRNG(x\oplus T_R\oplus PRNG(R_t)) \quad (۲۲)$$

پ) برچسب‌خوان به سرور ابری: برچسب‌خوان پس از دریافت M_{T1},M_{T2},M_{T3} مقادیر M_{R1} و M_{R2} طبق روابط (۲۳) و (۲۴) محاسبه می‌نماید. بدین‌ترتیب سرور ابری اعتبار برچسب‌خوان را به کمک M_{R2} تعیین می‌کند. پس از انجام محاسبات، برچسب‌خوان مقادیر $M_{R1},M_{R2},M_{T1}, M_{T2}, T_R$ را به محیط ابری می‌فرستد.

$$M_{R1}=Rot(T_R,SRID)\oplus SRID \quad (۲۲)$$

$$M_{R2}=PRNG\ (y' \oplus T_R) \quad (۲۳)$$

ت) سرور ابری به برچسب‌خوان: پس از دریافت $M_{R1},M_{R2},M_{T1}, M_{T2}, T_R$ توسط سرور ابری، در ابتدا وجود رابطه $T_{th1} < T_S - T_R < T_{th2}$ بررسی می‌شود. در صورت برقراری این شرایط، سرور ابری مقدار SRID را از جدول داده‌های شاخص شده برچسب‌خوان جستجو می‌کند تا مقدار تطبیقی برای M_{R1} یافت شود. در صورت وجود تطابق، سرور ابری مقدار y' متناظر را استخراج می‌کند و M_{R2} را طبق رابطه (۲۳) محاسبه می‌کند و درستی آن را بررسی می‌کند. در صورت درستی M_{R2}، آنگاه سرور ابری اعتبار برچسب‌خوان را تایید می‌کند. سپس مقدار SID در جدول داده‌های شاخص برچسب جستجو می‌شود. هدف یافتن تطبیق برای M_{T1} و M_{T2} است. در صورت وجود تطبیق، سرور ابری x' مربوطه را بازیابی و به همراه زمان فعلی (T_C) و $PRNG(R_T)$ به برچسب‌خوان ارسال می‌کند.

ث) برچسب‌خوان به برچسب : برچسب‌خوان چهار راه‌حل x_1، x_2، x_3 و x_4 را بر اساس x' ، p، q بدست می‌آورد. سپس براساس این راه‌حل مقدارM_{T3}' را طبق رابطه (۲۲) محاسبه تا برابری $M_{T3}'= M_{T3}$ حاصل و مقدار $x=x_i$ صحیح بدست‌آید. در چنین شرایطی برچسب احراز هویت شده‌است. برچسب‌خوان مقادیر T_C و M_{T4} را برای برچسب می‌فرستد.

$$M_{T4}= PRNG\ (x\oplus T_c) \quad (۲۴)$$

پس از دریافت M_{T4} و T_C توسط برچسب، در ابتدا اعتبار برچسب‌خوان با بررسی درستی M_{T4} تعیین می‌شود. در صورت درستی M_{T4}، هویت برچسب‌خوان به عنوان برچسب‌خوان مجاز به اثبات می‌رسد. در حقیقت صرفاً برچسب‌خوان مجاز با برخورداری از مقادیر p و q قادر به یافتن x از روی x' است. در این شرایط احراز هویت دو طرفه انجام شده‌است و مرحله به‌روزرسانی آغاز می‌شود.

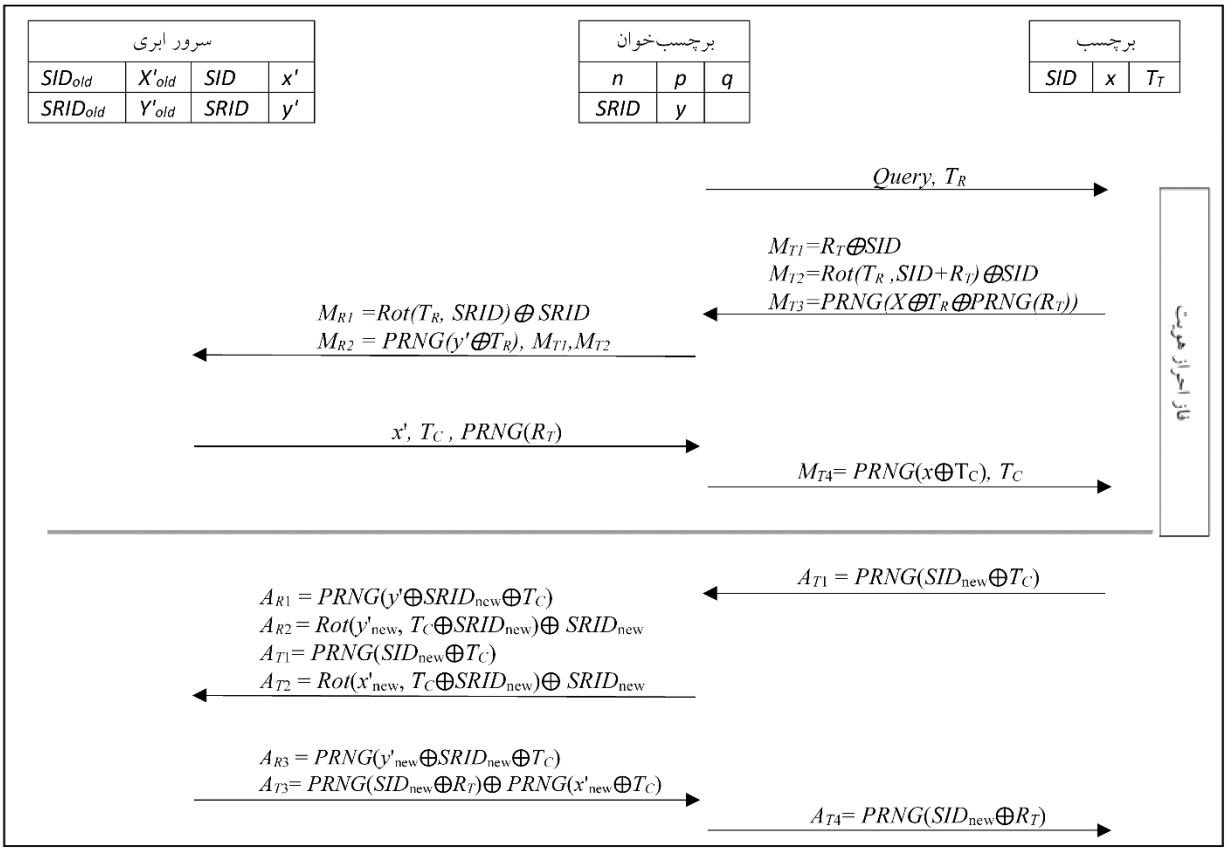
مرحله به روزرسانی

ج) برچسب به برچسب‌خوان: برچسب با استفاده از روابط (۲۵) و (۲۶)، مقادیر SID_{new} و x_{new} را محاسبه می‌کند. سپس مقدار A_{T1} را طبق رابطه (۲۷) محاسبه و به سمت برچسب‌خوان انتقال می‌دهد تا اطلاع‌رسانی به‌روزرسانی به سرور ابری ارسال شود.

$$SID_{new} = SID+T_C+R_t \quad (۲۵)$$

$$x_{new} = Rot(x, T_C) \oplus T_C \quad (۲۶)$$

$$A_{T1} = PRNG(SID_{new} \oplus T_C) \quad (۲۷)$$



شکل (۲): پروتکل احراز هویت LRAMP

چ) برچسب‌خوان به سرور ابری: پس از دریافت A_{T1}، به منظور به‌روزرسانی داده‌های برچسب در سرور ابری، برچسب‌خوان مقدار x_{new} را ازطریق رابطه (۲۶) محاسبه و x'_{new} را طبق رابطه (۲۸) محاسبه می‌کند. علاوه بر این مقادیر $SRID_{new}$، y_{new} و y'_{new} طبق روابط (۲۹) الی (۳۲) محاسبه شده تا داده‌های برچسب‌خوان نیز در سرور ابری به‌روزرسانی شوند.

$$x'_{new} = x^2_{new} \bmod n \quad (۲۹)$$

$$SRID_{new} = SRID + T_C \quad (۳۰)$$

$$y_{new} = Rot(T_C, y) \quad (۳۱)$$

$$y'_{new} = y^2_{new} \bmod n \quad (۳۲)$$

در ادامه برچسب‌خوان مقادیر جدید را به صورت مخفی از طریق A_{R1}، A_{R2} ، A_{T1} و A_{T2} که طبق روابط (۳۳) الی (۳۶) محاسبه می‌شوند، برای سرور ابری ارسال می‌نماید.

$$A_{R1} = PRNG(y'_{new} \oplus SRID_{new} \oplus T_C) \quad (۳۳)$$

$$A_{R2} = Rot(y'_{new}, T_C \oplus SRID_{new}) \oplus SRID_{new} \quad (۳۴)$$

$$A_{T1} = PRNG(SID_{new} \oplus T_C) \quad (۳۵)$$

$$A_{T2} = Rot(x'_{new}, T_C \oplus SRID_{new}) \oplus SRID_{new} \quad (۳۶)$$

ح) سرور ابری به برچسب‌خوان: پس از اینکه سرور ابری مقادیر $A_{T1}, A_{T2}, A_{R1}, A_{R2}$ را دریافت می‌کند، مقدار $SRID_{new}$ را به عنوان اولین گام محاسبه می‌کند. سپس سرور ابری صحت A_{R1} دریافتی را بررسی می‌کند. در صورت درستی A_{R1}، سرور ابری مقدار y'_{new} را از A_{R2} دریافت کرده و به‌روزرسانی جدول داده‌های شاخص برچسب‌خوان را به کمک مقادیر جدید آغاز می‌نماید. در صورتی‌که مقادیر SRID و y' از طریق داده‌های قدیمی جدول شاخص قابل دسترسی باشند، سرور ابری به‌روزرسانی را به‌صورت $SRID_{new} \rightarrow SRID$ و $y'_{new} \rightarrow y'$ اجرا می‌کند. از طرفی دیگر مقادیر $SRID_{old}$ و y'_{old} به صورت مقادیر قبلی باقی می‌مانند. در صورتی که SRID و y' در بخش داده‌های جدید جدول شاخص یافت گردند، سرور ابری امکان به‌روزرسانی $SRID \rightarrow SRID_{old}$، $y' \rightarrow y'_{old}$ ، $SRID_{new} \rightarrow SRID$ ، y'_{new}

$y' \rightarrow$ را فراهم می‌سازد. به طریق مشابه، سرور ابری مقدار SID_{new} را محاسبه می‌کند و سپس درستی مقدار A_{T1} دریافتی را بررسی می‌نماید. در صورت برقراری چنین شرایطی، سرور ابری مقدار x'_{new} را از A_{T2} دریافت می‌کند و جدول داده‌های شاخص برچسب را با مقادیر جدید به‌روزرسانی می‌کند. در صورت یافتن SID و x' در مقادیر قدیمی جدول شاخص، سرور ابری به‌روزرسانی را به‌صورت $SID_{new} \rightarrow SID$ و $x'_{new} \rightarrow x'$ اجرا می‌کند. این در حالیست‌که SID_{old} و x'_{old} ثابت باقی می‌مانند. در صورتی که مقادیر SID و x' در بخش داده‌های جدید جدول شاخص وجود داشته باشند، سرور ابری به‌روزرسانی‌ها را به‌صورت $SID \rightarrow SID_{old}$ و $x' \rightarrow x'_{old}$ ، $SID_{new} \rightarrow SID$ را اجرا می‌سازد. در نهایت سرور ابری مقدار A_{R3} و A_{T3} را طبق روابط (۳۷) و (۳۸) محاسبه و به‌عنوان پاسخ به سمت برچسب‌خوان ارسال می‌کند.

$$A_{R3} = PRNG(y'_{new} \oplus SRID_{new} \oplus T_C) \quad (۳۷)$$

$$A_{T3} = PRNG(SID_{new} \oplus R_t) \oplus PRNG(x'_{new} \oplus T_C) \quad (۳۸)$$

خ) برچسب‌خوان به برچسب: پس از دریافت A_{T3} و A_{R3} توسط برچسب‌خوان، در ابتدا درستی A_{R3} بررسی می‌شود. در صورت صحت A_{R3}، برچسب‌خوان درک می‌کند سرور ابری جدول داده‌های شاخص برچسب‌خوان را با موفقیت به‌روزرسانی کرده و در ادامه برچسب‌خوان نیز مقادیر $SRID_{new}$ و y_{new} را با SRID و y جایگزین می‌کند. علاوه بر این، برچسب‌خوان مقدار A_{T4} را طبق رابطه (۳۹) محاسبه می‌کند و آن را برای برچسب می‌فرستد.

$$A_{T4} = A_{T3} \oplus PRNG(x'_{new} \oplus T_C) \quad (۳۹)$$

پس از دریافت A_{T4} توسط برچسب، صحت درستی A_{T4} بررسی می‌گردد. در صورت درستی A_{T4}، برچسب می‌فهمد سرور ابری با موفقیت جدول داده‌های شاخص برچسب را به‌روزرسانی کرده‌است. سپس برچسب مقادیر SID_{new} و x_{new} را جایگزین SID و x می‌کند. در انتها برچسب مقدار T_C را با T_T جایگزین می‌نماید.

۶- تحلیل امنیتی پروتکل اصلاح شده

در این قسمت امنیت پروتکل پیشنهادی تجزیه و تحلیل قرار می‌شود و مشخص می‌گردد که چگونه کمبودهای امنیتی پروتکل فان و همکارانش برطرف شده‌است.

۶-۱- مقاومت در برابر حمله افشای پارامترهای مخفی

داده‌های مخفی برچسب که در این پروتکل بکار رفته‌اند عبارتند از SID و x. هر دو مقدار قبل از ارسال روی کانال غیرامن رمزنگاری می‌شوند. در صورتی‌که مهاجم خواهان دسترسی به x باشد، ضروری است تا مقدار x را از روی PRNG(x) یا x' بدست بیاورد. در حالت اول، مهاجم نمی‌تواند مقدار مدنظر را بدست بیاورد زیرا PRNG() یک عملیات امن به شمار می‌رود. در حالت دوم، با توجه به مساله فاکتورگیری از اعداد بزرگ، دسترسی مهاجم به x غیرممکن است چرا که یکی از دو مقدار p و q مجهول است. علاوه‌براین، با توجه به مقدار نامشخص R_T، مهاجم برای بدست‌آوردن SID از روی $Rot(T_R, SID+R_T) \oplus SID$ با مشکل روبرو می‌شود. SID و x' ذخیره شده در سرور ابری نیز داده‌های محرمانه را افزایش نمی‌دهند. لذا در روش پیشنهادی، ناشناس بودن برچسب تضمین می‌شود.

۶-۲- مقاومت در برابر حمله ردیابی

در پروتکل LRAMP از تکنیک تمبر زمانی در سمت برچسب استفاده شده است. بدین ترتیب برچسب اعتبار تمبر زمانی را براساس معادله $T_R > T_T$ تست می‌کند و سپس پارامترهای امنیتی مورد نیاز را محاسبه می‌کند. در صورت وجود تمبر زمانی غیرمعتبر، پروتکل اتصال را قطع می‌کند. از طرف دیگر در پایان هرجلسه نیز مقادیر SID و x به‌روزرسانی می‌شوند. علاوه بر این، برچسب در تولید مقادیر M_{T1}، M_{T2} و M_{T3} از عدد تصادفی جدید (R_t) استفاده می‌کند. بدین ترتیب پاسخ‌های برچسب نه پیوسته هستند و نه توسط مهاجم قابل پیش‌بینی می‌باشند. بنابراین وی قادر به ردیابی برچسب هدف نیست.

۶-۳- امنیت روبه‌جلو و روبه‌عقب

در پروتکل LRAMP، تمامی پیام‌ها به‌وسیله توابع معکوس‌ناپذیر Rot (.) و PRNG() محاسبه می‌شوند. بدین‌ترتیب هیچ پیامی وجود نخواهد داشت که مهاجم بتواند برای آن به اطلاعات محرمانه فعلی و قبلی دسترسی پیدا کند. از طرفی پیام‌ها در این پروتکل به

نحوی تولید می‌شوند که نمی‌توان این پیام‌ها را به جلسات قبل یا بعد مرتبط ساخت زیرا در همگی آن‌ها از اعداد تصادفی جدید بهره برده شده‌است. بدین ترتیب روش پیشنهادی امنیت روبه‌جلو و روبه‌عقب را تضمین می‌کند.

۶-۴- مقاومت در برابر حمله ناهمزمان‌سازی

در صورتی‌که فرض بر این شود که مهاجم قادر به مسدودسازی آخرین پیام پروتکل باشد و تحت این وضعیت برچسب چندتایی (SID و x) و برچسب‌خوان چندتایی (SRID و y) را برای اجرای حمله ناهمزمان‌سازی به‌روزرسانی نکند، با این‌وجود سرور چندتایی (SID_{old},x'_{old},SID_{new},x'_{new}) و ($SRID_{old}$,y'_{old},$SRID_{new}$,y'_{new}) را ذخیره می‌کند و با استفاده از SID_{old} و x_{old} برچسب را مورد تایید قرار می‌دهد و با استفاده از $SRID_{old}$ و y_{old} برچسب‌خوان را مورد تایید قرار می‌دهد. علاوه‌براین در این پروتکل وجود R_T در پیام‌های M_{T2} و M_{T3} باعث شده که امکان تولید پیام‌هایی مشابه وجود نداشته باشد. در این صورت مهاجم نمی‌تواند پیام M_{T4} تولید کند. بدین‌ترتیب مهاجم قادر نیست برچسب، برچسب‌خوان و سرور را وارد حالت ناهمزمان نماید.

۶-۵- مقاومت در برابر حمله تکرار

در روش LRAMP، تمامی پیام‌ها به‌وسیله اعداد تصادفی جدیداً تولید شده T_R و R_T تولید می‌شوند. بدین ترتیب مهاجم قادر به تکرار پیام‌های استراق‌سمع شده از نشست های قبلی نیست و نمی‌تواند هویت‌های موجود در پروتکل را فریب دهد. بدین ترتیب پروتکل مذکور در برابر حملات تکرار مقاوم می‌شود.

۶-۶- مقاومت در برابر حمله جعل هویت برچسب

مهاجم قادر نیست پاسخ مورد انتظار را به برچسب‌خوان تولید و ارسال نماید. علت این است که تمبر زمانی (T_R) تولید شده توسط برچسب‌خوان در پیام‌های برچسب وجود دارد و فرآیند احراز هویت در سمت سرور چنین امکانی را از وی سلب می‌کند. بدین ترتیب پروتکل LRAMP در برابر حمله جعل هویت برچسب مقاوم است.

۶-۷- مقاومت در برابر حمله جعل هویت برچسب‌خوان

در پروتکل LRAMP، برچسب‌خوان با استفاده از تمبر زمانی T_C و R_T مقادیر M_{T4} و A_{T4} را محاسبه می‌کند. بدین ترتیب عامل مهاجم قادر به تکرار پیام های استراق سمع شده M_{T4} و A_{T4} از نشست قبلی نیست. و لذا نمی‌تواند برچسب را فریب بدهد.

در جدول (۲) پروتکل LRAMP در مقابل حملات یاد شده با پروتکل پیشین خود و نیز چند پروتکل که از نظر انتقال پیام‌ها ساختار مشابهی با این پروتکل دارند و سازگار با استاندارد EPC-C1G2 می‌باشند از نظر امنیتی مقایسه شده است.

۷- تحلیل امنیتی رسمی پروتکل LRAPM

در زمان طراحی پروتکل، به مجموعه‌ای از روش‌های تحلیلی نیاز است که با استفاده از آنها بتوان تحلیل درستی از امنیت پروتکل را داشته و فرایند طراحی پروتکل را به‌طور صحیح پیش‌برد. تحلیل رسمی پروتکل‌های امنیتی، روشی رسمی برای تحلیل پروتکل‌های امنیتی است که براساس آن برآورده شدن اهداف امنیتی یک پروتکل بررسی می‌گردد. یکی از روش‌های متداول تحلیل رسمی استفاده از منطق BAN است. در این بخش، سطح امنیتی پروتکل LRAPM براساس روش رسمی مبتنی بر منطق BAN ارزیابی می‌شود .تجزیه و تحلیل یک پروتکل با استفاده از منطق BAN در ۵ مرحله انجام می‌شود: مرحله (۱) توصیف پیام‌های پروتکل، مرحله (۲) ایده‌آل کردن پیام‌های پروتکل، مرحله (۳) بیان فرضیات صریح، مرحله (۴) ارائه اهداف امنیتی پیشنهادی طرح، مرحله (۵) اثبات اهداف پیشنهادی. نمادهای استفاده شده در روش اثبات مبتنی بر منطق BAN در جدول (۳) نشان داده شده است.

جدول (۲): مقایسه چند پروتکل احراز هویت با طرح LRAMP

پروتکل LRAMP	پروتکل *fan* [۸]	پروتکل *Tewari &Gupta* [۱۵]	پروتکل *fan* [۱۸]	پروتکل *Benssalah* [۲۸]	پروتکل
✓	✓	X	✓	✓	مقاوم در برابر افشای پارامترهای مخفی
✓	X	✓	X	X	مقاوم در برابر حمله ردیابی
✓	✓	✓	✓	✓	امنیت روبه‌جلو و روبه عقب
✓	X	✓	✓	X	مقاوم در برابر حمله ناهمزمان‌سازی
✓	✓	✓	✓	✓	مقاوم در برابر حمله تکرار
✓	✓	✓	X	X	مقاوم در برابر حمله جعل هویت برچسب
✓	X	✓	X	✓	مقاوم در برابر حمله جعل هویت برچسب‌خوان

جدول (۳): علامت‌های اختصاری به‌کاررفته در منطق BAN

توضیحات	علامت اختصاری
P مقدار X را تایید می‌کند	$P \mid\equiv X$
P مقدار X را دریافت می‌کند	$P \lhd X$
P مقدار X را ارسال می‌کند	$P \mid\sim X$
X جدید است	$\#(X)$
X با کلید رمزی K رمزنگاری می‌شود	$\{X\}_K$
P و Q دارای کلید رمزی اشتراکی X هستند	$P \overset{X}{\rightleftharpoons} Q$
اگر P آنگاه Q	$\frac{P}{Q}$

منطق BAN از ۱۹ قانون تشکیل شده‌است. در این اثبات از سه قانون آن استفاده می‌شود که به شرح زیر بیان شده است:

- قانون (R1) – $\frac{P \mid\equiv P \overset{Y}{\rightleftharpoons} Q \,.\, P \lhd \{X\}_Y}{P \mid\equiv Q \mid\sim X}$: این قانون بدین معنی است که اگر P معتقد است که Y راز مشترک بین P و Q است و اگر P باور دارد که پیام $\{X\}_Y$ را دریافت کرده‌است، بنابراین P معتقد است که Q پیام X را ارسال کرده‌است.
- قانون (R2) – $\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X\,.\,Y)}$: این قانون بدان معنا است که اگر P معتقد است که پیام X جدید است، آنگاه او می‌پذیرد که مجموعه پیام (X, Y) جدید است.
- قانون (R3) – $\frac{P \mid\equiv Q \mid\sim (X.Y)}{P \mid\equiv Q \mid\sim (X)}$: این قانون به این معنی است که اگر P معتقد است که Q مجموعه پیام (X, Y) را ارسال کرده‌است، P می‌پذیرد که Q پیام X را ارسال کرده‌است.

اثبات پروتکل LRAPM بر اساس منطق BAN به شرح زیر است:

مرحله ۱ (تعریف پیام‌های پروتکل): در این مرحله پیام‌های بین برچسب و برچسب‌خوان در پروتکل LRAPM به شکل روابط ریاضی بیان می‌شوند.

PM1 : $(R \rightarrow T) : \{Query , T_R\}$
PM2 : $(T \rightarrow R) : \{R_T \oplus SID , Rot (T_R, SID + R_T) \oplus SID , PRNG (T_R \oplus x \oplus PRNG(R_T)\}$
PM3 : $(R \rightarrow C) : \{R_T \oplus SID , Rot (T_R, SID + R_T) \oplus SID , PRNG (T_R \oplus x \oplus PRNG(R_T) , Rot (T_R, SRID) \oplus SRID , PRNG (T_R \oplus y')\}$
PM4 : $(C \rightarrow R) : \{x' , T_C, PRNG (R_T) \}$
PM5 : $(R \rightarrow T) : \{ PRNG (x \oplus T_C) , T_C \}$
PM6 : $(T \rightarrow R) : \{ PRNG (SID_{new} \oplus T_C) \}$
PM7 : $(R \rightarrow C) : \{ PRNG (y' \oplus SRID_{new} \oplus T_C) , Rot (y'_{new} , T_C \oplus SRID_{new}) \oplus SRID_{new} , PRNG (SID_{new} \oplus T_C) , Rot (x'_{new} , T_C \oplus SRID_{new}) \oplus SRID_{new} \}$
PM8 : $(C \rightarrow R) : \{ PRNG (y'_{new} \oplus SRID_{new} \oplus T_C) , PRNG (SID_{new} \oplus R_T) \oplus PRNG(x'_{new} \oplus T_C) \}$
PM9 : $(R \rightarrow T) : \{ PRNG (SID_{new} \oplus R_T) \}$

مرحله ۲ (ایده‌آل‌سازی پیام‌های پروتکل): در این مرحله پیام‌های پروتکل LRAPM، مطابق علائم اختصاری منطق BAN به حالت ایده‌آل تبدیل می‌شوند.

IM1 : $(R \rightarrow T) : T \lhd \{Query , T_R\}$
IM2 : $(T \rightarrow R) : R \lhd \{R_T \oplus SID , Rot (T_R, SID + R_T) \oplus SID , PRNG (T_R \oplus x \oplus PRNG(R_T)\}$
IM3 : $(R \rightarrow C) : C \lhd \{R_T \oplus SID , Rot (T_R, SID + R_T) \oplus SID , PRNG (T_R \oplus x \oplus PRNG(R_T) , Rot (T_R, SRID) \oplus SRID , PRNG (T_R \oplus y')\}$
IM4 : $(C \rightarrow R) : R \lhd \{x' , T_C, PRNG (R_T) \}$
IM5 : $(R \rightarrow T) : T \lhd \{ PRNG (x \oplus T_C) , T_C \}$
IM6 : $(T \rightarrow R) : R \lhd \{ PRNG (SID_{new} \oplus T_C) \}$
IM7 : $(R \rightarrow C) : C \lhd \{ PRNG (y' \oplus SRID_{new} \oplus T_C) , Rot (y'_{new} , T_C \oplus SRID_{new}) \oplus SRID_{new} , PRNG (SID_{new} \oplus T_C) , Rot (x'_{new} , T_C \oplus SRID_{new}) \oplus SRID_{new} \}$
IM8 : $(C \rightarrow R) : R \lhd \{ PRNG (y'_{new} \oplus SRID_{new} \oplus T_C) , PRNG (SID_{new} \oplus R_T) \oplus PRNG(x'_{new} \oplus T_C) \}$
IM9 : $(R \rightarrow T) : T \lhd \{ PRNG (SID_{new} \oplus R_T) \}$

مرحله ۳ (فرضیات صریح): فرضیات صریح اولیه پروتکل LRAPM به شرح زیر بیان می‌شوند:

A1: $R \mid\equiv \#(T_R)$
A2: $T \mid\equiv \#(R_T)$
A3: $C \mid\equiv \#(T_C)$
A4: $C \mid\equiv C \overset{SID}{\rightleftharpoons} T$
A5: $T \mid\equiv T \overset{SID}{\rightleftharpoons} C$
A6: $R \mid\equiv R \overset{SRID}{\rightleftharpoons} C$
A7: $C \mid\equiv C \overset{SRID}{\rightleftharpoons} R$
A8: $T \mid\equiv T \overset{x}{\rightleftharpoons} R$
A9: $R \mid\equiv R \overset{x}{\rightleftharpoons} T$

مرحله ۴ (اهداف امنیتی پروتکل LRAPM): در اینجا اهداف پروتکل پیشنهادی به شرح زیر فهرست‌بندی می‌شوند.

G1: $C \mid\equiv R \mid\sim y'$
G2: $C \mid\equiv T \mid\sim R_T$
G3: $R \mid\equiv T \mid\sim T_R$
G4: $T \mid\equiv R \mid\sim T_C$
G5 : $C \mid\equiv R \mid\sim y'_{new}$
G6 : $C \mid\equiv T \mid\sim T_C$
G7 : $R \mid\equiv C \mid\sim y'_{new}$
G8: $T \mid\equiv C \mid\sim R_T$

مرحله ۵ (فرآیند اثبات) : در بخش فعلی، سطح امنیتی پروتکل با اعمال قوانین منطقی BAN تجزیه و تحلیل می‌شود.

نتیجه ۱: طبق پیام IM3، فرضیات A1 و A7 وبراساس قوانین R1 و R3 می‌توان نتیجه گرفت که $C \mid\equiv R \mid\sim y'$.

نتیجه ۲: طبق پیام IM3، فرضیات A2 و A4 وبراساس قوانین R1 و R3 می‌توان نتیجه گرفت که $C \mid\equiv T \mid\sim R_T$.

نتیجه ۳: طبق پیام IM2، فرض A1 و براساس قانون R2 می‌توان نتیجه گرفت که $R \mid\equiv \# \{ PRNG (T_R \oplus x \oplus PRNG(R_T) \}$. بنابراین طبق پیام‌های IM4 و IM2، فرضیات A1 و A9 و براساس قوانین R1 و R3 می‌توان نتیجه گرفت که $R \mid\equiv T \mid\sim T_R$.

نتیجه ۴: طبق پیام IM5، فرض A8 و براساس قوانین R1 و R3 می‌توان نتیجه گرفت که $T \mid\equiv R \mid\sim T_C$.

نتیجه ۵: طبق پیام IM7، فرضیات A1 و A7 وبراساس قوانین R1 و R3 می‌توان نتیجه گرفت که $C \mid\equiv R \mid\sim y'_{new}$.

نتیجه ۶: طبق پیام IM7، فرضیات A2 و A4 وبراساس قوانین R1 و R3 می‌توان نتیجه گرفت که $C \mid\equiv T \mid\sim T_C$.

نتیجه ۷: طبق پیام IM8، فرضیات A3 و A6 وبراساس قوانین R1 و R3 می‌توان نتیجه گرفت که $R \mid\equiv C \mid\sim y'_{new}$.

نتیجه ۸: طبق پیام IM9، فرض A2 و براساس قانون R2 می‌توان نتیجه گرفت که $T \mid\equiv \# PRNG (SID_{new} \oplus R_T) \}$. بنابراین طبق پیام‌های IM9، فرضیات A2 و A5 و براساس قوانین R1 و R3 می‌توان نتیجه گرفت که $T \mid\equiv C \mid\sim R_T$.

بر اساس نتایج بالا، مشاهده می‌شود که تمامی اهداف امنیتی پروتکل LRAPM برآورده شده‌است.

۸- ارزیابی عملکرد پروتکل LRAPM

در این بخش عملکرد و کارایی پروتکل LRAPM با مقایسه این طرح با طرح‌های مشابه خود مشخص می‌گردد. جدول (۴) مقایسه کارایی طرح LRAPM در مؤلفه برچسب با مرتبط‌ترین پروتکل‌های سبک‌وزن مانند پروتکل ULRMAPC، پروتکل عقیلی و همکارانش و پروتکل فان و همکارانش را نشان می‌دهد. مقایسه‌ها نشان از آن دارد که LRAPM هنوز به اندازه کافی کارآمد است. در طرح احراز هویت ULRMAPC، برچسب مقادیر IDS، ID، K و Tt را ذخیره می‌کند .بنابراین، فضای ذخیره‌سازی در برچسب ۴L است .در پروتکل عقیلی و همکارانش فضای ذخیره‌سازی برچسب ۵L است، در این طرح برچسب IDS، ID، K، Tt و s_0 را ذخیره می‌کند. در پروتکل فان و همکارانش، فضای ذخیره‌سازی در برچسب ۲L است. در طرح فان و همکارانش برچسب SID و X را ذخیره می‌کند .در پروتکل LRAPM فضای ذخیره سازی در برچسب ۳L است که در آن برچسب مقادیر SID, X, T_T را ذخیره می‌کند.

جدول (۴): مقایسه عملکرد پروتکل LRAPM با پروتکل‌های ULRMAPC، عقیلی و همکارانش و فان و همکارانش

پروتکل	عملیات‌های محاسباتی برچسب	اندازه حافظه موردنیاز برچسب
ULRMAPC	RG^2, +, ⊕, Rot^2	۴L
عقیلی و همکارانش	RG,+,⊕,Rot^2	۴L
فان و همکارانش	⊕, + ,Rot, PRNG	۲L
LRAPM	Tr,RG,⊕, Rot,$PRNG^2$	۳L

جدول (۵) مقایسه هزینه‌ها و بارهای ارتباطی پروتکل LRAPM را با سایر پروتکل‌های مشابه نشان می‌دهد. هزینه‌های ارتباطی پروتکل LRAPM بیشتر از سه پروتکل دیگر است. لازم به ذکر است که افزایش هزینه‌های ارتباطی اجتناب‌ناپذیر است. طرح LRAPM قادر به ایمن‌سازی سیستم‌های اینترنت اشیاء پزشکی براساس فناوری RFID مبتنی بر سرور ابری است. در چنین سیستم‌هایی، کانال ارتباطی بین برچسب‌خوان و سرور ابری قانونی ناامن فرض می‌شود. لازم به ذکر است که در پروتکل‌های ULRMAPC و عقیلی اگرچه برچسب-خوان‌ها سیار در نظر گرفته شده است اما ارتباط در محیط ابری امن صورت می‌گیرد. پروتکل پیشنهادی با وجود داشتن پیام‌های بیشتر نسبت به پروتکل فان و همکاران، سطح امنیت بالاتری را ارائه می‌کند. بنابراین مشاهده می‌شود که کارایی پروتکل پیشنهادی در سیستم‌های RFID موبایلی مبتنی بر ابر بهتر از سه پروتکل فوق است. روش LRAPM همچنین برای اطمینان از الزامات امنیت و حریم خصوصی خدمات مراقبت بهداشتی RFID مبتنی بر ابر بسیار مناسب است.

جدول (۵): مقایسه هزینه و بار ارتباطی در پروتکل LRAPM با پروتکل‌های ULRMAPC، عقیلی و همکارانش و فان و همکارانش

پروتکل	برچسب	برچسب‌خوان	سرور ابری	مجموع
ULRMAPC	$۳l_p$	$۲l_t + ۲l_p$	$۲l_p$	$۲l_t + ۷l_p$
عقیلی و همکارانش	$۲l_p$	$۲l_t + ۲l_p$	$۲l_p$	$۲l_t + ۶l_p$
فان و همکارانش	$۳l_p$	$۲l_t + ۷l_p$	$l_m + l_t + ۲l_p$	$l_m + ۳l_t + ۱۲l_p$
LRAPM	$۴l_p$	$۲l_t + ۷l_p$	$l_m + l_t + ۳l_p$	$l_m + ۳l_t + ۱۴l_p$

l_p طول ID و اعداد تصادفی است. l_m طول خروجی باقیمانده اعداد درجه ۲ است و l_t نشان دهنده طول زمان است.

۹- نتیجه گیری

در این مقاله ، امنیت پروتکل احراز هویت را که توسط فان و همکاران که برای اینترنت پزشکی اشیاء (MIoT) در فضای ابری پیشنهاد شده است، ارزیابی شد. آنها ادعا کردند که طرح آنها از امنیت بالایی برخوردار است. با این حال، در این مقاله، ثابت گردید که طرح آنها در برابر حملات تکرار، جعل هویت برچسب‌خوان، ردیابی برچسب‌ها و حمله ناهمزمان‌سازی آسیب پذیر است. علاوه بر این، در جهت بهبود پروتکل یاد شده، پروتکل جدیدی با نام LRAPM ارائه شد که با سیستم‌های مراقبت بهداشتی RFID مبتنی بر فضای ابری سازگار باشد. پروتکل LRAPM به اندازه کافی در برابر حملات شناخته شده مقاوم است. مقایسه پروتکل LRAPM با پروتکل های مشابه از نظر امنیت، هزینه‌های محاسباتی، ذخیره‌سازی و ارتباطاتی نشان می‌دهد که پروتکل LRAPM بالاترین سطح امنیت را در مقایسه با طرح‌های

مشابه دارد. لازم به ذکر است که افزایش هزینه‌های محاسباتی و ارتباطی در پروتکل LRAPM نسبت به پروتکل فان، سرعت برچسب را اندکی کاهش می‌دهد. اما این کاهش سرعت در برابر امنیت حاصله قابل چشم‌پوشی است. این پروتکل همچنان می‌تواند برای استفاده در سیستم‌های RFID ارزان‌قیمت سازگار با سیستم‌های MIOT پیاده‌سازی شود.

مراجع

[1] A. Satoh, and K. Takano, "A scalable dual-field elliptic curve cryptographic processor." *IEEE Transactions on Computers*, 52(4), pp.449-460, 2003. doi: 10.1109/TC.2003.1190586.

[2] A. Juels, "RFID security and privacy: A research survey". *IEEE journal on selected areas in communications*, 24(2), pp.381-394,2006. doi: 10.1109/JSAC.2005.861395 .

[3] R. Weinstein, "RFID: a technical overview and its application to the enterprise." *IT professional*, 7(3), pp.27-33, 2005. doi: 10.1109/MITP.2005.69 .

[4] I. Erguler, "A potential weakness in RFID-based Internet-of-things systems." *Pervasive and Mobile Computing*, 20, pp.115-126, 2015. https://doi.org/10.1016/j.pmcj.2014.11.001.

[5] S. Karthikeyan, and M. Nesterenko, "RFID security without extensive cryptography.", *In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, (pp. 63-67), 2005. https://doi.org/10.1145/1102219.1102229.

[6] M. Shariq, K. Singh, M.Y. Bajuri, A.A. Pantelous, A. Ahmadian, and M. Salimi, "A secure and reliable RFID authentication protocol using digital schnorr cryptosystem for IoT-enabled healthcare in COVID-19 scenario." *Sustainable Cities and Society*, 75, p.103354, 2021. doi:https://doi.org/10.1016/j.scs.2021.103354

[7] Z. Shi, J. Pieprzyk, C. Doche, Y. Xia, Y. Zhang, and J. Dai, "A strong lightweight authentication protocol for low-cost RFID systems.", *International Journal of Security and Its Applications*, 8(6), pp.225-234, 2014. doi: 10.14257/ijsia.2014.8.6.20.

[8] K. Fan, S. Zhu, K. Zhang, H. Li, and Y. Yang, "A lightweight authentication scheme for cloud-based RFID healthcare systems." *IEEE Network*, 33(2), pp.44-49, 2019. doi: 10.1109/MNET.2019.1800225.

[9] T.C. Yeh, Y. J. Wang, T.C. Kuo, and S. S. Wang, "Securing RFID systems conforming to EPC Class 1 Generation 2 standard.", *Expert systems with applications*, 37(12), pp.7678-7683, 2010. https://doi.org/10.1016/j.eswa.2010.04.074.

[10] M. H. Habibi, M. R. Alagheband, and M. R. Aref, "June. Attacks on a lightweight mutual authentication protocol under EPC C-1 G-2 standard.", *In IFIP International Workshop on Information Security Theory and Practices* (pp. 254-263). Springer, Berlin, Heidelberg, 2011. doi: https://doi.org/10.1007/978-3-642-21040-2_18.

[11] M. Mohammadi, M. Hosseinzadeh and M. Esmaeildoust, "Analysis and improvement of the lightweight mutual authentication protocol under EPC C-1 G-2 standard," *Advances in Computer Science: An International Journal (ACSIJ)*, vol. 3, pp. 10-16, 2014.

[12] S.M. Alavi, K. Baghery and B. Abdolmaleki, "Security and Privacy Flaws in a Recent Authentication Protocol for EPC C1 G2 RFID Tags", *ACSIJ Advances in Computer Science: An International Journal*, Vol. 3, Issue 5, No.11, pp.44-52, 2014. doi: https://doi.org/10.1007/s11277-015-2469-0.

[13] C. Caballero-Gil, P. Caballero-Gil, A. Peinado-Domı´nguez, & J. Molina-Gil, "Lightweight authentication for RFID used in VANETs", *In Computer aided systems theory–EUROCAST*, pp. 493–500, 2012. doi: https://doi.org/10.1007/978-3-642-27579-1_64.

[14] F. Moradi, H. Mala, B. Tork-Ladani, "Security Analysis and Strengthening of an RFID Lightweight Authentication Protocol Suitable for VANETs", *Wireless Personal Communications, ed: springer*, pp 2607-2621, 2015. doi: https://doi.org/10.1007/s11277-015-2558-0.

[15] A. Tewari, and B. B. Gupta, "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags." *The Journal of Supercomputing*, 73(3), pp.1085-1102, 2017. doi: https://doi.org/10.1007/s11227-016-1849-x.

[16] M. Safkhani, and N. Bagheri, "Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things." *The Journal of Supercomputing*, 73(8), pp.3579-3585, 2017. doi: https://doi.org/10.1007/s11227-017-1959-0.

[17] K. H. Wang, C. M. Chen, W. Fang, and T. Y. Wu, "On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags." *The Journal of Supercomputing*, 74(1), pp.65-70, 2018, doi: https://doi.org/10.1007/s11227-017-2105-8

[18] K. Fan, Y. Gong, C. Liang, H. Li, and Y. Yang, "Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G," *Security and Communication Networks*, 9(16), pp.3095-3104, 2016. doi: https://doi.org/10.1002/sec.1314.

[19] C. T. Li, C. C. Lee, C. Y. Weng, and C. M. Chen, 2018. "Towards secure authenticating of cache in the reader for RFID-based IoT systems,", *Peer-to-Peer Networking and Applications*, 11(1), pp.198-208, 2018. doi: https://doi.org/10.1007/s12083-017-0564-6

[20] K. Srivastava, A. K. Awasthi, S. D. Kaul, and R. C. Mittal, "A hash based mutual RFID tag authentication protocol in telecare medicine information system,", *Journal of medical systems*, 39(1), pp.1-5, 2015, doi: https://doi.org/10.1007/s10916-014-0153-7.

[21] C. T. Li, C. Y. Weng, and C. C. Lee, "A secure RFID tag authentication protocol with privacy preserving in telecare medicine information system," *Journal of medical systems*, 39(8), pp.1-8, 2015. doi: https://doi.org/10.1007/s10916-015-0260-0.

[22] S. S. S. GhaemMaghami, M. Mirmohseni, A. Haghbin, "A privacy preserving improvement for SRTA in telecare systems." *arXiv preprint arXiv:1510.04197*, 2015. doi: https://doi.org/10.48550/arXiv.1510.04197

[23] D. He, N. Kumar, N. Chilamkurti, and J.H. Lee, "Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol". Journal of medical systems, 38(10), pp.1-6, 2014. doi: https://doi.org/10.1007/s10916-014-0116-z.

[24] C. I. Lee, and H. Y. Chien, "An elliptic curve cryptography-based RFID authentication securing e-health system," *International Journal of Distributed Sensor Networks*, 11(12), p.642425, 2015. doi: https://doi.org/10.1155/2015/642425.

[25] N. Kumar, K. Kaur, S. C. Misra, and R. Iqbal, "An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud," *Peer-to-Peer Networking and Applications*, 9(5), pp.824-840, 2016. doi: https://doi.org/10.1007/s12083-015-0332-4.

[26] C. Jin, C. Xu, X. Zhang, and F. Li, "A secure ECC-based RFID mutual authentication protocol to enhance patient medication safety," *Journal of medical systems*, 40(1), pp.1-6, 2016. doi: https://doi.org/10.1007/s10916-015-0362-8.

[27] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, and J. Shen, "A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications," *Journal of Ambient Intelligence and Humanized Computing*, 9(4), pp.919-930, 2018. doi: https://doi.org/10.1007/s12652-017-0485-5.

[28] M. Benssalah, M. Djeddou, and K. Drouiche, "Security enhancement of the authenticated RFID security mechanism based on chaotic maps," *Security and Communication Networks*, 7(12), pp.2356-2372, 2014. doi: https://doi.org/10.1002/sec.946.

[1] Internet of Things
[2] real-time disease management
[3] medical Internet of Things
[4] Radio Frequency Identification
[5] lightweight RFID authentication protocol for MIoT systems