1st Conference on
ENGINEERING & INNOVATION
December 2-3, 2020 - University of Tabriz
NCEI
ENGINEERING & INNOVATION
اولین کنفرانس
مهندسی و فن آوری
۱۲ و ۱۳ آذر ماه ۱۳۹۹ - دانشگاه تبریز
ISC
مجوز پایگاه استنادی علوم جهان اسلام ۹۹۲۰۰-۶۷۱۰۷

بهبود امنیت اطّلاعات در شبکهٔ اینترنت اشیا با بهره‌گیری از الگوریتم زنجیره‌ای

شهرام جمالی[1]، نوید عباپور[2]*، رسول محبوب[3]

1- استاد گروه مهندسی برق و کامپیوتر، دانشگاه محقق اردبیلی، اردبیل، jamali@uma.ac.ir

2- دانشجوی مقطع کارشناسی گروه علوم کامپیوتر، دانشگاه محقق اردبیلی، اردبیل، navidabapour@gmail.com

3- دانشجوی مقطع کارشناسی گروه علوم کامپیوتر، دانشگاه محقق اردبیلی، اردبیل، rasoulmahboub@gmail.com

چکیده

گسترش موازی حجم عظیمی از اطّلاعات با تکنولوژی های ارتباطی، موجب شده تا اهمّیّت حفاظت از داده‌های متنوّع در فضای سایبری و جوامع مختلف افزایش یابد و نیاز برجسته‌ای به امنیت اطّلاعات در حیطه‌های نظامی، مالی، مخابراتی و ارتباطی احساس شود که درنتیجهٔ این نیازها، چالش‌های گوناگونی در سر راه سیستم‌های اطّلاعاتی و ارتباطی قرار می‌گیرند که از جملهٔ این چالش‌های برجسته می‌توان به حفظ تناسب بین سطح امنیت و عملکرد پروتکل‌ها اشاره کرد. همچنین یکی دیگر از چالش‌های موجود در زمینهٔ سیستم های هوشمند، انتقال یک‌پارچهٔ سیستم‌های قدیمی و راه‌اندازی آنان بر اساس اینترنت اشیا است. از سوی دیگر، اطمینان از سازگاری و انعطاف‌پذیری در ادغام دستگاه‌های موجود با اینترنت اشیا ضروری است. در این اثر، با استفاده از الگوریتم زنجیره ای درهم‌سازی(هش) روشی جهت کنترل دسترسی، احراز هویت و ذخیره و بازیابی اطّلاعات کاربران در اینترنت اشیا ارائه شده است که کاربران می توانند با امنیت خاطر بیشتری نسبت به روش های مشابه و بدون اطّلاع از طریق و مکان ذخیره‌سازی، داده هایشان را به سرورهای ذخیره‌سازی اینترنت اشیا بسپارند.

واژه‌های کلیدی: معماری امنیت، رمزنگاری، امنیت اینترنت اشیا، اصالت سنجی

1- مقدمه

امنیت و حریم شخصی دو نگرانی عمدهٔ سازمان‌های نوین امروزی به‌شمار می‌روند. در دنیای شبکه های کامپیوتری، محیط مجازی اجازه می‌دهد تا دسترسی کاربر به قدرت محاسباتی، بیش از دسترسی موجود وی در دنیای فیزیکی باشد. برای ورود به این محیط مجازی کاربر موظّف است نسبت به انتقال داده‌ها در سراسر شبکه اقدام نماید[4]. همان‌طور که بشر به‌سوی مدل اینترنتی شبکه های اشیا درحرکت می‌باشد، نیازمند به تأکید زیادی نسبت به امنیت اطّلاعات و حریم خصوصی می‌باشد. از دست رفتن اطّلاعات یا فاش شدن آن‌ها می‌تواند ضربات شدید و جبران ناپذیری به کسب‌وکار، برند و اعتبار یک سازمان وارد کند.

پیشگیری از فاش شدن اطّلاعات باید به‌عنوان عاملی مهم در نظر گرفته شود[5]. تهدیدات امنیتی بر روی کاربران شبکه اینترنت اشیا به دودستهٔ داخلی و خارجی تقسیم‌بندی می‌شوند. تهدیدهای داخلی به این معنی هستند که مشتریان داده‌های مهم و حیاتی خود را در فضای شبکه اینترنت اشیاء میزبان ذخیره می‌کنند و کارکنان سازمان به علّت داشتن دسترسی به این داده‌ها از اطّلاعات مشتریان

سوء استفاده کنند[6]. باوجوداینکه تهدیدهای داخلی برای ارائه‌دهندگان شبکهٔ اینترنت اشیا یک تهدید بزرگ است ولی تهدیدهای خارجی هم می‌توانند تأثیر بسیار زیادی داشته و باعث بروز خسارت‌هایی به سیستم و فرآیندهای آن شوند. نقاط ضعف یک سازمان ارائه‌دهنده می‌توانند راهی برای مهاجمان خارج از سازمان بازکرده و باعث حملات مخرّب خارجی شوند. بنابراین رایانش ابری باوجود داشتن مزایای زیاد، همواره دارای تهدیدات امنیتی بی‌شماری برای اطّلاعات در حال تبادل است که باعث می‌شود مشتریان از بهره بردن از مزایای شبکه اینترنت اشیا باز بمانند[7]. از بین تمام جنبه‌های اینترنت اشیا، جنبهٔ امنیت قابل توجه بسیاری از محققان بوده و روش‌های زیادی را برای آن ذکر کرده‌اند و پروژه‌های بسیاری نیز در این زمینه انجام شده است که هریک دارای مزایا و معایبی است و لذا تحقیقات در این زمینه همچنان ادامه دارد[2].

برچسب های RFID بر اساس منبع انرژی تأمین کننده به سه دسته فعّال، غیرفعّال، نیمه فعّال تقسیم می شوند. برچسب های فعّال، شامل باتری‌هایی است که انرژی آنها را تأمین می کند. برچسب‌های غیرفعّال انرژی خود را از سیگنال‌هایی که برچسب خوان ارسال می‌کند دریافت می کنند. برچسب های نیمه فعّال علاوه بر استفاده از باطری داخلی می‌توانند از انرژی منتقل شده توسّط برچسب خوان نیز بهره‌مند شوند[3،4]. جهت تامین امنیت در RFID تاکنون فناوری‌های مختلفی به منظور شناسایی خودکار طراحی و پیاده سازی شده‌اند. کدهای میله‌ای، کارت‌های هوشمند، تشخیص صدا، برخی فناوری های بیومتریک و OCR نمونه هایی در این زمینه می باشند[6].

امروزه از RFID در بسیاری از برنامه های کاربردی برای شناسایی و ردیابی کالاها و دارایی‌ها استفاده می‌شود. یکی دیگر از موارد کاربرد این دستگاه‌ها در شبکه اینترنت اشیا می‌باشد. در این تکنولوژی نیز، امنیت دارای اهمّیّت خاصی می‌باشد[6]. از بین تمام جنبه های اینترنت اشیا، جنبهٔ امنیتی قابل توجه بسیاری از محققان بوده و روش های زیادی را برای آن ذکر کرده اند و پروژه های بسیاری نیز در این زمینه انجام شده است که هریک دارای مزایا و معایبی است و لذا تحقیقات در این زمینه همچنان ادامه دارد. جهت ارزیابی کارایی برنامه‌های امنیتی، موارد زیر در نظر گرفته می‌شوند[7]:

- محرمانگی: یعنی اطمینان داشته باشیم که فقط مالکین رمز یا افراد مجاز به اطّلاعات دسترسی دارند.
- احراز هویت: اصالت سنجی یا کسب اطمینان از اینکه هویت طرف دوم رابطه اثبات شود.
- جامعیّت: حفظ تمامیّت یا اینکه اطّلاعات در حین انتقال تغییر نمی کنند.
- کنترل دستیابی یا اینکه استفاده غیر مجاز نداشته باشیم.

ساده ترین راهکار احراز هویت که بسیاری از کاربران از آن استفاده کرده اند، ساختار سادهٔ یک کلید احراز هویت متنی است که ما آن را به عنوان پسورد یا رمز عبور می شناسیم و برای احراز هویت شدن در سیستم های مختلف از آن استفاده می کنیم. امّا احراز هویت به تنهایی شامل فاکتورهای مختلفی است که برای بالا بردن سطح امنیتی باید آنها را رعایت کرد[8].

2- سوابق پژوهش

تاکنون چندین پروتکل بر اساس تکنیک های رمزنگاری پیشنهاد شده که در ادامه اشاره ای مختصر بر آنها خواهد شد:

در اثر عملی [11] یک طرح ساده و مقیاس پذیر با قیمت پایین که مبتنی بر عملیات Hash می باشد، برای حل مسائل امنیتی و حفظ حریم خصوصی پیشنهاد شده است که از آن تحت عنوان پروتکل SRFID یاد می شود. این طرح، یک احراز هویت متقابل دو گامه بین پایگاه داده و برچسب فراهم کرده و نیاز به کانال امن بین برچسب خوان و پایگاه داده برای تکمیل فرایند احراز هویت ندارد. پایگاه داده همهٔ اطلاعات مرتبط با برچسب ها را ذخیره می کند و محتوای برچسب‌ها به وسیلهٔ یک شناسهٔ منحصر به فرد شاخص گذاری می‌شوند. برچسب، شناسهٔ فعلی خودش را به برچسب خوان منتقل می‌کند که برچسب خوان، همان مقدار را به پایگاه داده تحت عنوان شاخص پایگاه داده ارسال می کند. احراز هویت بر اساس اشتراک دو مقدار سرّی بین برچسب و پایگاه داده می باشد و بعد از یک احراز هویت متقابل موفّق، شناسهٔ برچسب به وسیلهٔ برچسب و پایگاه داده به روزرسانی می شود که امنیت ارسال برای سیستم

را فراهم می کند. این طرح امنیتی مانع حملاتی همچون استراق سمع، حملات ارسال مجدد، تکثیر و ردیابی تگ، انکار یا محروم سازی از سرویس و MITM می‌شود.

پژوهشگران در مقالهٔ [12] یک پروتکل احراز هویت متقابل مبتنی بر هش(Hash) را به عنوان راه‌حلی برای مسائل حریم خصوصی و جعل داده پیشنهاد کرده‌اند. این پروتکل برای ارسال یک مقدار تصادفی تولید شده به وسیلهٔ برچسب به پایگاه داده طراحی شده است. همچنین در این پروتکل، مقدار تصادفی با یک مقدار سرّی و پنهانی جایگزین شده و در یک پیغام پاسخ به کار گرفته می شود. ویژگی پروتکل پیشنهادی، تولید ثابت پیغام هایی با پاسخ مشخّص و بدون واسط از درخواست های تولید شدهٔ مورد انتظار توسط مهاجم است. این پروتکل در برابر حملاتی چون استراق سمع، ارسال مجدد، تکثیر تگ، جعل داده، MITM و به ویژه حمله تجزیه و تحلیل ترافیک و نفوذ سریع، امن است.

در مقالهٔ [13] پروتکل احراز هویتی مبتنی بر مسئله ECDLP ارائه شده است. دراین پروتکل، مقادیر s و p به ترتیب کلید خصوصی وکلیدعمومی برچسب‌اند. در این پروتکل، برچسب یک عدد تصادفی همچون r1 را تولید می‌کند و مقدار r1P=M1 را برای سرویس دهنده می‌فرستد. سرویس دهنده با دریافت مقدارM1، یک عدد تصادفی همچون r2 را تولید کرده و برای برچسب می‌فرستد. برچسب با دریافت مقدار r2، مقدار r1+sr2=M2 را برای سرویس دهنده بر می‌گرداند. سرویس دهنده مقدار M2P+r2Z را محاسبه می‌کند و برابری این مقدار را با M1 بررسی می‌کند که اگر برابری درست باشد، برچسب به رسمیت شناخته می‌شود. این پروتکل می تواند از حملهٔ جعل کردن جلوگیری کند ولی ازحملهٔ فیزیکی و مردمیانی(MITM) رنج می‌برد.

نویسندگان اثر [14] یک پروتکل احراز هویت RFID را ارائه کرده‌اند که در این پروتکل وقتی سرویس دهنده، برچسب را به چالش می‌کشد، برچسب دوعدد تصادفی r1 و r2 را تولیدکرده ومقدار r2P+r1P1=M1 را به سرویس دهنده پس می‌فرستد. سرویس دهنده به محض دریافت مقدار M1، یک عدد تصادفی مثل r3 را تولید کرده و به برچسب می‌فرستد. برچسب با دریافت این عدد، مقادیر r3s1+r1=M2 وr3s2+r2=M3 را محاسبه و به سرویس دهنده باز می‌گرداند. سرویس دهنده مقدار r3Z+M3P2+M2P1 را محاسبه کرده و برابری آن را با M1 بررسی می‌کند. اگر برابری درست بود، برچسب را می‌پذیرد. این پروتکل از حملات جعل، مردمیانی(MITM) و حملهٔ فیزیکی رنج می برد.

در اثر علمی [15] یک پروتکل اعتبارسنجی ارائه شده است که مختص گره های سیّار و متحرّک است. در این پروتکل برای برقراری ارتباط گره های سیّار در ابتدا باید توسط خوشه‌ای منتخب اعتبارسنجی شوند. در این روش، یک پیام در خواست معتبر ارسال شده و در پاسخ، گیرنده یک پیام اعتبارسنجی معتبر را دریافت می‌کند. برای اثبات خواص حفظ حریم در این روش، از فرموله سازی در دیفرانسیل استفاده کرده‌اند که این روش به نسبت پروتکل‌هایی مانند هش پایه و OSK دارای سربار ارتباطی کمتر و امنیت بیشتر و حفظ حریم خصوصی بیشتری است.

در منبع [16] یک پروتکل ارتباطی برای سیستم های RFID در اینترنت اشیا پیشنهاد شده است که امنیت در آن به وسیله اوراکل تصادفی مهیا می‌شود. در این مدل که SPAP نام دارد، اشیا دارای یک EPC منحصربه‌فرد بوده و از رمزنگاری متقارن، تابع هش یک‌طرفه و XOR استفاده می‌شود. این روش اعتبارسنجی دوطرفه و امنیت داخلی را برقرار کرده و در برابر برخی حملات پایه نیز مقاومت می‌کند.

محققان در [17] روش اعتبارسنجی مبتنی بر ABC را برای ادراک اینترنت اشیا پیشنهاد کرده‌اند. در این معماری کاربر به عنوان ناظر لایهٔ ادراک برای دستگاه‌هایی مانند تلفن همراه و کامپیوترهای هوشمند می‌باشد. در این روش کارایی بهتری را می‌توان روی گره های حسگر به نسبت مابقی پروتکل ها مشاهده کرد.

در مقالهٔ [18] از دو پروتکل HAC و RAC استفاده کرده‌اند و در این روش، دسترسی به تگ را با استفاده از تابع هش یک‌طرفه با قفل گذاری و یا گشودن قفل کنترل کرده‌اند.

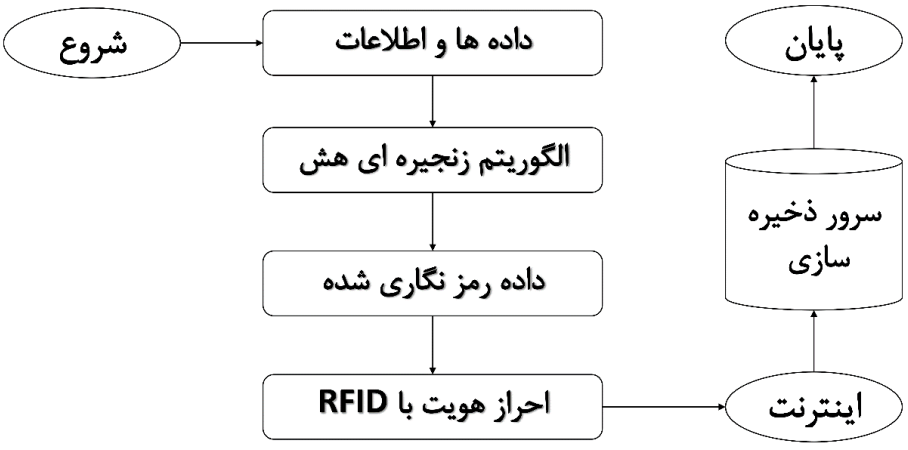
پژوهشگران اثر [19] در طرحی برای احراز هویت، برای اختفای بیشتر از تگ موقعیت استفاده کرده‌اند. توابع دیگری که در این طرح استفاده شده است عبارتند از: تابع هش یک‌طرفه و عملیات باینری.

در منبع [20] برای حفاظت سیستم در مقابل ردیابی، از رهگیری رو به عقب استفاده کرده‌اند که در این طرح شناسه تگ هر زمان که گزارش داده شود، با استفاده از یک مکانیزم زنجیره ای هش کم هزینه به روزرسانی می‌شود.

3- روش پیشنهادی

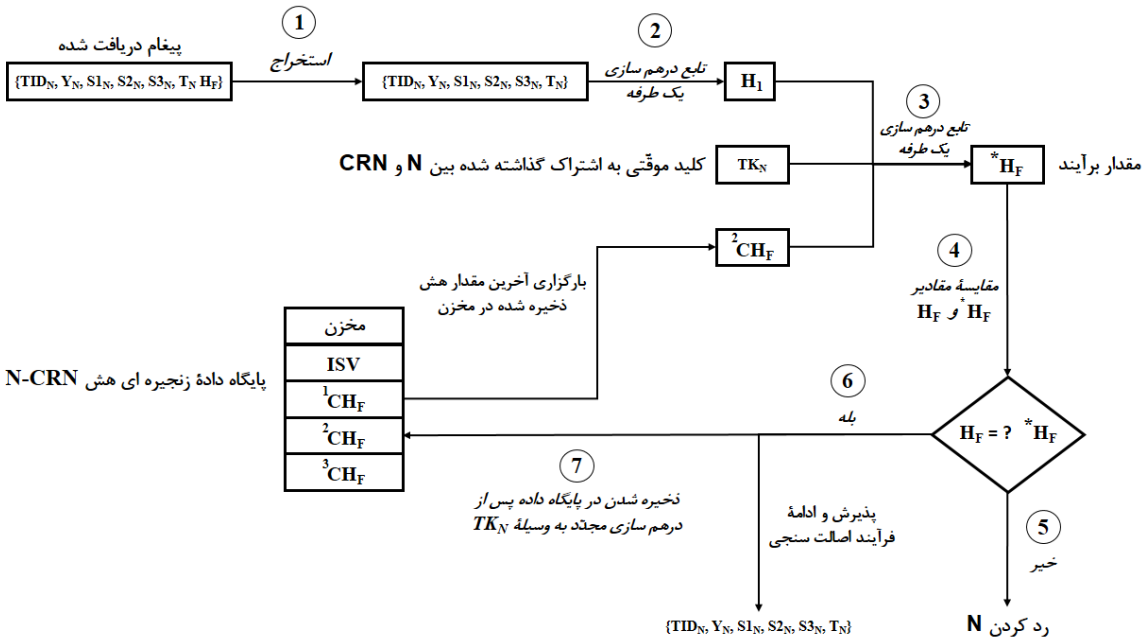
رمزنگاری زنجیره ای هش به جای یک کلید از زوج کلید، همانند رمزگذاری متقارن، استفاده می کند. این رمزگذاری تک کلیدی بین دو طرف، مستلزم این است که هر دو طرف کلید سرّی داشته باشند. بدین ترتیب با بالارفتن تعداد دسته ها، تعداد کلیدها نیز بیشتر می شود. علاوه بر این، توزیع کلید مخفی با بیشتر شدن تعداد کلیدها تقریباً غیرقابل کنترل می‌شود. البتّه استفادهٔ بلندمدت از یک کلید مخفی برای هر زوج باعث می شود که این عملکرد در مقابل حملات آنالیز رمزی آسیب پذیر شود. برای مقابله با این مشکلات لاینحل، تسهیل توزیع کلید در رمزنگاری زنجیره ای هش متقارن، آن هم زمانی که با حجم بالایی از داده‌های حاوی رشته‌های باینری و صفر و یک سر و کار داریم، به وجود آمد.

در روش پیشنهادی ابتدا، سرویس دهنده عدد تصادفی را ایجاد می کند. سپس کاربر با کلید عمومی اش داده ها را رمزنگاری کرده و به همراه تگ به سمت سرویس دهنده ارسال می کند. در سمت سرویس دهنده، الحاق الگو های تگ با داده رمز شده انجام می شود. سرور پس از دریافت اطلاعات ارسالی چکیده را اول با کلید خصوصی خودش سپس با کلید عمومی فرستنده از رمز خارج می کند، اگر با کلید عمومی فرستنده که اطلاعات را ارسال کرده اطلاعات از رمز خارج شد، فرستنده هویتش تایید می شود. سپس سرور داده های رمز شده با الگوهای تگ را به بخش های کوچکتری شکسته و به صورت نرمال روی چند سرور ذخیره سازی توزیع می کند. داده ها در سرورهای ذخیره سازی توزیع شده ذخیره می شوند. در این تحقیق بهبود احراز هویت و کنترل دسترسی در اینترنت اشیاء ارائه خواهد شد در روش پیشنهادی رمزنگاری در سرورهای ذخیره سازی ابری با الگوریتم زنجیره ای هش انجام می گردد ، سپس از ترکیب یک نوع رمزنگاری زنجیره ای هش استفاده می شود، در این روش برای از نهان نگاری استفاده خواهیم کرد که امنیت بالایی داشته باشد(شکل 1).



شکل1: مراحل کلی روش پیشنهادی

همچنین روش پیشنهادی برای ذخیره سازی امن اطلاعات در شکل (2) آمده است و همانطور که می‌توان مشاهده کرد، داده ها در سمت کاربر رمزنگاری زنجیره ای هش شده و به همراه تگ به سرویس دهنده ارسال می‌شوند و سرویس دهنده داده‌های دریافتی را در سرورهای ذخیره سازی، بارگذاری می‌کند. یکی از بخش های مهم روش پیشنهادی برای افزایش محرمانگی، استفاده از الگوریتم رمزنگاری زنجیره‌ای هش مناسب است که می تواند به شکل چشمگیری در حفظ محرمانگی اطّلاعات موثّر واقع شود. در ادامه، نحوهٔ رمزنگاری زنجیره ای هش داده ها و بارگذاری آن ها در سمت سرویس دهنده توضیح داده می شود.

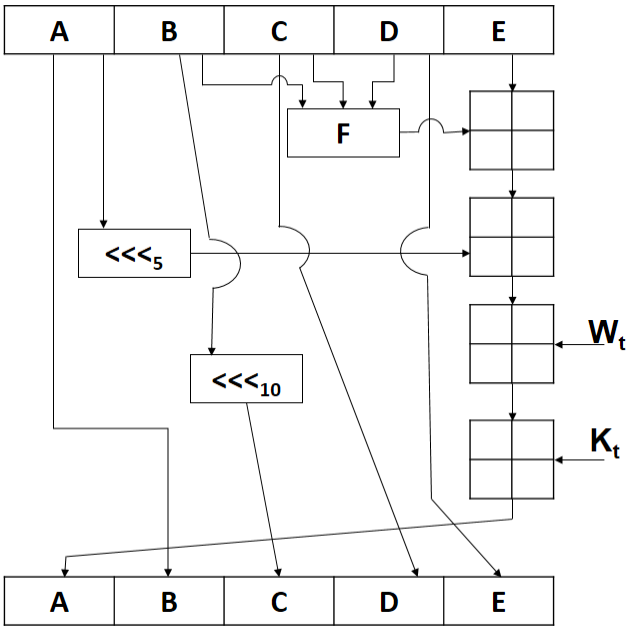


شکل2: روند بهره‌برداری از الگوریتم زنجیره ای هش[13]

درواقع در روش پیشنهادی، رمزنگاری زنجیره‌ای هش در سمت سرویس گیرنده(کاربر) انجام می‌گردد و رمزگشایی در سمت سرویس گیرنده باعث می‌شود تا دیگر مشکل گلوگاه، که از بزرگترین چالش‌های موجود در اینترنت اشیا است، را نداشته باشیم و همچنین بار کاری سرور کاهش می‌یابد.

4- بهره‌برداری از الگوریتم زنجیره ای هش

الگوریتم زنجیره‌ای درهم‌سازی ایمن از نوع 0(SHA-0)، دارای قدرت ایمنی بالاتری نسبت به سایر الگوریتم های خانوادهٔ خود است. به همین دلیل می‌توان از آن برای محاسبهٔ چکیدهٔ یک پیام یا فایل که به عنوان ورودی به الگوریتم ارائه می‌شود استفاده کرد. در این الگوریتم، پیام تقسیم بر تکه می‌شود و اندازهٔ هر تکه برابر با 512 بیت است. هر کدام از این تکه ها، با شناسایی پنج بافر A، B، C، D و E پردازش می‌شود. مراحل این نوع از الگوریتم زنجیره ای در ادامه توضیح داده شده.



شکل3: الگوریتم زنجیره ای هش[13]

4-1- مقداردهی اوّلیّهٔ متغیّرها

h0 = 0x67452301
h1 = 0xEFCDAB89
h2 = 0x98BADCFE
h3 = 0x10325476
h4 = 0xC3D2E1F0
m = طول پیام (بر حسب بیت)

4-2- پیش‌پردازش

در این مرحله یک بیت " 1" به پیام افزوده می‌شود. به عنوان مثال اگر طول پیام از یک رشتهٔ چند برابر 8 بیتی تشکیل شده، 0x80 را اضافه می کند. اضافه کردن $0 \geq k > 512$ بیت '0'، به طوری که طول پیام حاصل بر حسب بیت، مطابق با $64 \equiv -448 \pmod{512}$ باشد؛ به عنوان مثال، یک عدد صحیح 64 بیتی بزرگ اضافه کند. بنابراین طول کلی چند برابر 512 بیت است.

4-3- پردازش پیام در 512 بیت متوالی

break message into 512-bit chunks
***for** each chunk*
break chunk into sixteen 32-bit big-endian words w[i], $0 \leq i \leq 15$

4-4- گسترش شانزده کلمهٔ 32 بیتی به هشت کلمهٔ 32 بیتی

```
for i from 16 to 79
   w[i] = (w[i-3] xor w[i-8] xor w[i-14] xor w[i-16]) leftrotate 1
```

5-4- وارد کردن مقدار هش برای هر تکه

```
a = h0
b = h1
c = h2
d = h3
e = h4
for i from 0 to 79
      if 0 ≤ i ≤ 19 then
         f = (b and c) or ((not b) and d)
         k = 0x5A827999
      else if 20 ≤ i ≤ 39
         f = b xor c xor d
         k = 0x6ED9EBA1
      else if 40 ≤ i ≤ 59
         f = (b and c) or (b and d) or (c and d)
         k = 0x8F1BBCDC
      else if 60 ≤ i ≤ 79
         f = b xor c xor d
         k = 0xCA62C1D6

      temp = (a leftrotate 5) + f + e + k + w[i]
      e = d
      d = c
      c = b leftrotate 30
      b = a
      a = temp
```

6-4- اعمال مقدار Hash Chunk

```
h0 = h0 + a
h1 = h1 + b
h2 = h2 + c
h3 = h3 + d
h4 = h4 + e
```

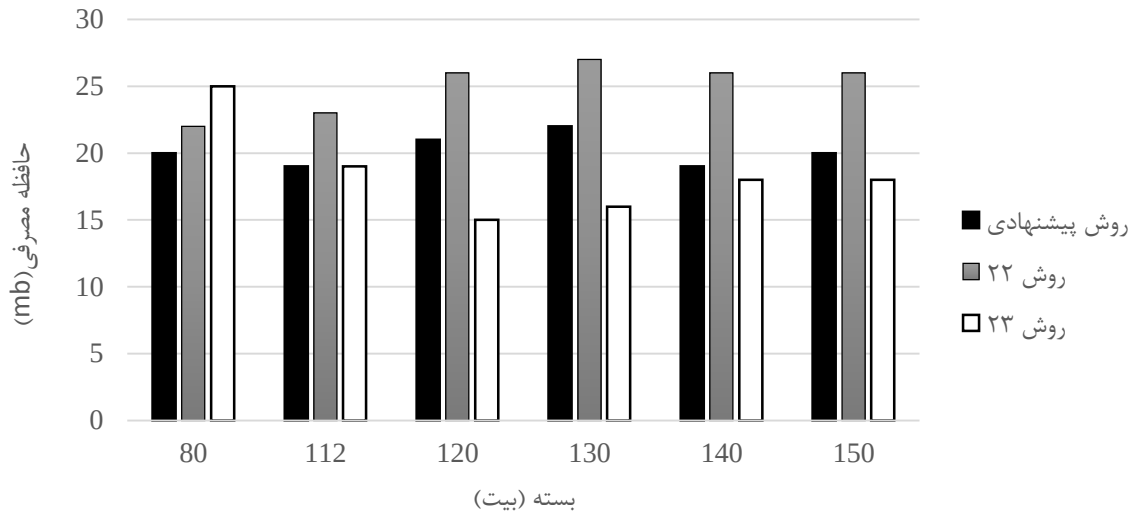
4-7- تولید مقدار نهایی هش، به صورت یک شمارهٔ 160 بیتی

hh = (h0 ***leftshift*** *128)* ***or*** *(h1* ***leftshift*** *96)* ***or*** *(h2* ***leftshift*** *64)* ***or*** *(h3* ***leftshift*** *32)* ***or*** *h4*

لازم به ذکر است که همهٔ متغیرها مقادیر 32 بیتی بدون تگ هستند و طول پیام 64 بیت و برای چکیدهٔ پیام مقدار 160 بیتی است. با در نظر داشتن اینکه از الگوریتم زنجیره‌ای هش، برای چکیده کردن پیام‌ها مثل پیام‌های 80 بیتی، 32 بیتی و... استفاده می شود و در مقدار هش برای چکیده‌سازی پیام‌ها از کلمات 32 بیتی استفاده می‌شود و خروجی حاصل یک پیام 160 بیتی است، برای هر کدام از پیام ها برچسب خاصی مثل G0، G1، G2، G3 در نظر گرفته می‌شود. علاوه بر این برای پیام ها متغیرکاری نیز در نظر گرفته می شود که با حروف مختلفی مثل a، b، c، d، e، f مشخص می گردند. در این نوع الگوریتم کلماتی که دارای مقادیر هش هستند با حرف H نشان داده می شوند مثل H0، H1، H2، H3، H4، H5 که حروفی که با H نشان داده می شوند مشخص می کند که این کلمات حاوی هش هستند. البتّه در الگوریتم اس اچ ای(درهم سازی ایمن) علاوه بر برچسب ها، متغیرهای کاری و مقادیر هش H از یک نوع کلمهٔ موقتی نیز استفاده می شود که آن را T می‌نامند.

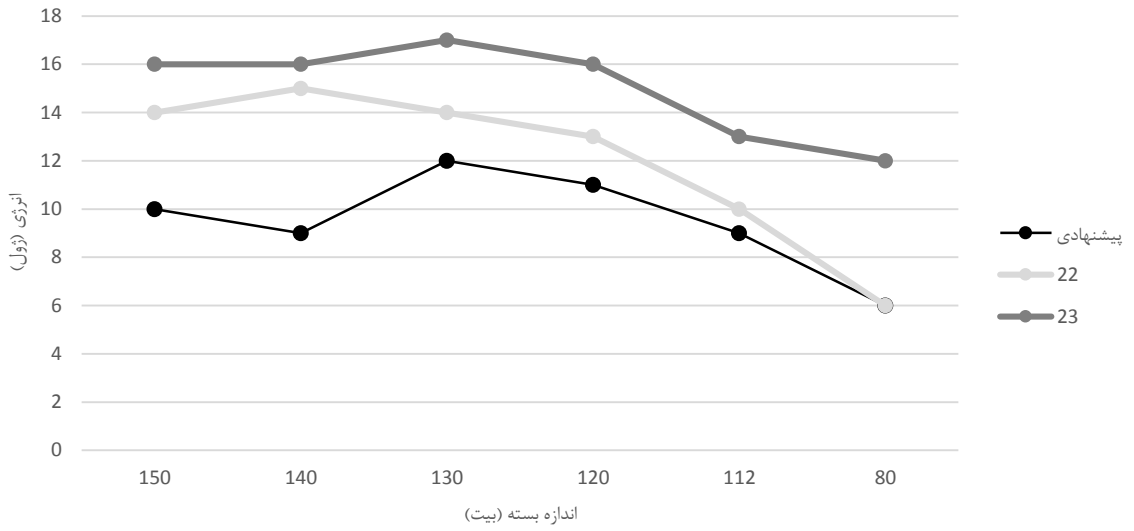
5- تحلیل نتایج

بررسی معیار حافظهٔ مصرفی: همانطور که در شکل (9) در این معیار میزان حافظه مصرفی (برحسب مگا بایت) بررسی شده است تا درخواستهای احرازهویت به طور کامل انجام شود. بر اساس تعداد بسته ها ارسالی مورد مقایسه قرار گرفته است، نتایج نشان می دهد که روش [23] به ازای بسته های بیشتر کمترین میزان مصرف حافظه را دارد و روش پیشنهادی نتوانسته است به ازای بسته های بالا حافظه مصرفی را کاهش دهد.



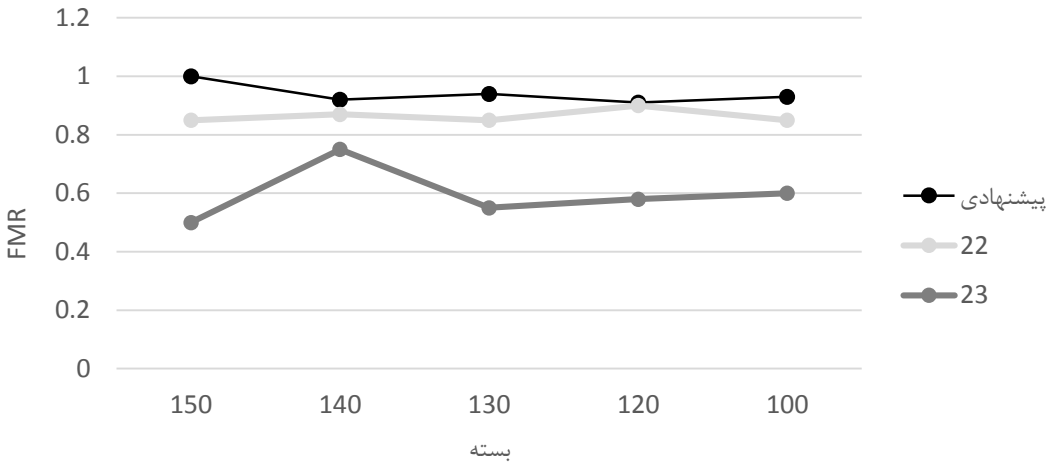
شکل4: حافظهٔ مصرفی

بررسی معیار انرژی مصرفی: در این معیار، مقدار انرژی مصرفی برای انتقال اطّلاعات از مبدا به مقصد تا درخواست‌های احرازهویت به طور کامل انجام شود مورد مقایسه قرار گرفته است، در هر مرحله تعداد بسته‌های مربوط به داده‌ها بیشتر شده است. همانطور که در شکل (5) قابل مشاهده است، روش پیشنهادی میزان انرژی مصرفی کمتری نسبت به روش های مشابه را به خود اختصاص داده است.



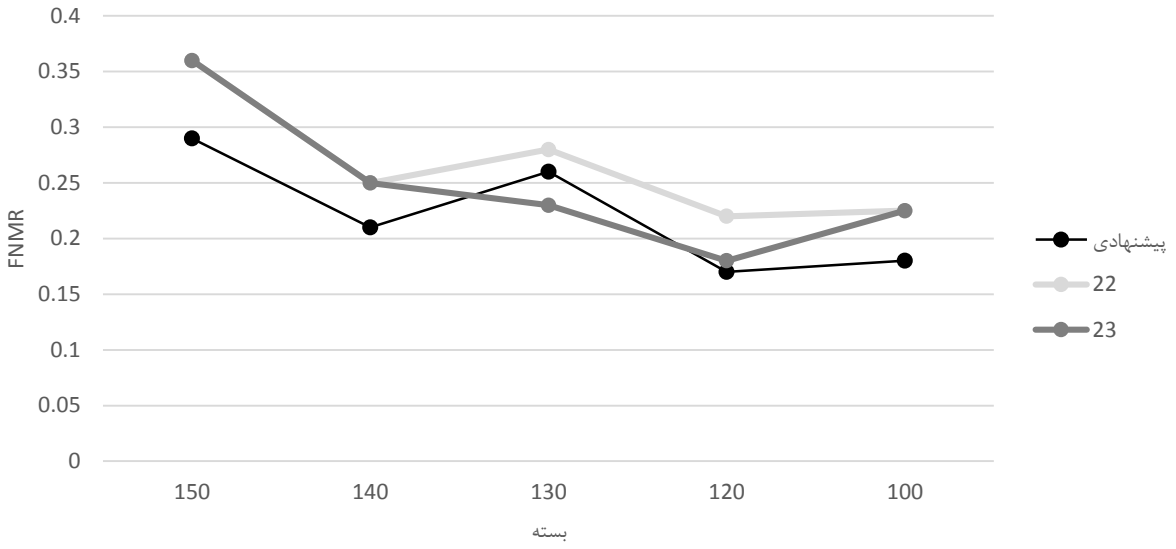
شکل5: انرژی لازم جهت انتقال درخواست

معیار FMR: نرخ تطابق جعلی یا FMR برابر است با احتمال قبول یک نمونه نادرست به‌عنوان نمونه‌ای اصلی. از این معیار به نسبت تصدیق نادرست یا FAR نیز یاد می‌شود. به بیان ساده‌تر، این معیار یعنی احتمال اینکه اثر فرد B به‌اشتباه به‌عنوان اثر فرد A شناخته شده باشد. در شکل (6) معیار FMR برای روش پیشنهادی و روش‌های [22] و [23] به ازای بسته‌های مختلف مورد ارزیابی قرار گرفته است.



شکل6: مقایسهٔ معیار FMR

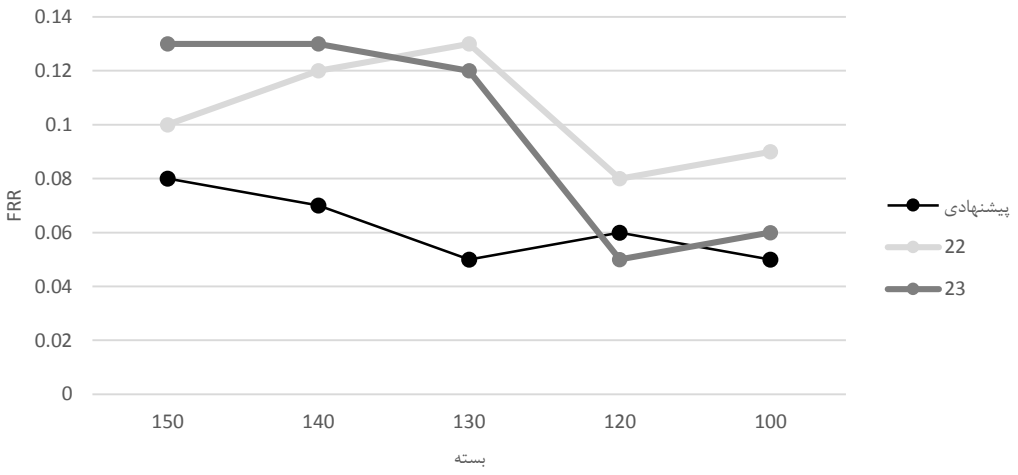
بررسی FNMR: معیار FNMR احتمال رد شدن اشتباه یک نمونه از فرد قانونی یا اصلی است . در بسیاری از موارد به FNMR به‌عنوان نسبت رد شدن نادرست یا FRR نیز اطلاق می‌شود. نتیجهٔ شبیه‌سازی برای معیار فوق و روش‌های [22] و [23] به ازای بسته های مختلف در شکل (7) نمایش داده شده است.



شکل7: مقایسهٔ معیار FNMR

با توجه به نتیجه شبیه سازی روش پیشنهادی فقط در 6 درصد مواقع دچار خطای FNMR می‌شود و نسبت به روش های قبلی عملکرد بهتری دارد.

معیار عدم پذیرش اشتباه: این خطا زمانی رخ می‌دهد که یک سیستم بیومتریک، کاربر دارای مجوز را به اشتباه نپذیرد . FRR یا False Reject Rate به معنی نرخ عدم پذیرش اشتباه که خطای شماره یک هم نامیده می‌شود و درصد دفعاتی که عدم پذیرش اشتباه رخ می‌دهد را نمایان می‌کند.



شکل8: مقایسهٔ معیار FRR

روش پیشنهادی به دلیل استفاده از رمزنگاری تصادفی باعث شده است که معیار عملکرد بسیار خوبی نسبت روش های [22] و [23] به ازای بسته های مختلف داشته باشد. لازم به ذکر است که در [22] و [23] اطّلاعات بصورت یکپارچه روی یک رسانهٔ ذخیره سازی، ذخیره می‌شوند که در صورت مورد حمله قرار گرفتن سرور، کل اطّلاعات فاش خواهند شد.

6- نتیجه‌گیری

برخی از روش های ذخیره سازی کل فایل را روی سرورها آپلود کرده و تنها رمز کردن محتویات فایل اکتفا می کنند. اینگونه روش ها به دلیل عدم شکست فایل، با مشکل جدّی روبرو خواهند بود. در صورتی که در روش پیشنهادی، قبل از شروع اپلود فایل، ابتدا آن فایل به بخش های کوچکتری شکسته می شود و اطّلاعات به بخش های کوچکتری شکسته شده و روی چندین رسانه توزیع می شوند. بدین شکل ریسک از بین رفتن اطلاعات کاهش می یابد و با مورد حمله قرار گرفتن یک سرور، کل اطلاعات فاش نخواهد شد. همچنین برای واکشی اطلاعات نیز چون اطلاعات همزمان از چندین سرور واکشی می شوند سرعت نیز بالا می رود. جدای از این موارد، در قسمت پردازش، چون اطلاعات به صورت رمزنگاری شده از سیستم سرویس گیرنده به سرور اینترنت اشیا ارسال می شود در حین ارسال اطلاعات نیز اخلالگران به اطلاعات دسترسی نخواهند داشت و با تبادل کلید با استفاده از RSA عملیات احراز هویت کاربر صورت خواهد گرفت.

مراجع

[1] Shiyong Zhang, Chen Gongliang, Yongkai Zhou, and Jianhua Li, ”Enhanced-Bivium Algorithm for RFID System” Mathematical Problems in Engineering, vol. 2015, Article ID 616182, 6 pages, 2015. doi:10.1155/2015/616182.

[2] Alizadeh M., Zamani M., Shahemabadi A. R., Shayan J. & Azanik A., A Survey on Attacks in RFID Networks, Open International Journal of Informatics, 1(1), 2013.

[3] Mitrokotsa A., Rieback M. R. & Tanenbaum A. S., Classifying RFID Attacks and Defenses. Information Systems Frontiers, 12(5), 2010

[4] Khedr W. I., SRFID: A Hash-based security scheme for low cost RFID systems, Egyptian Informatics Journal, 14(1), 2013.

[5] Cho J. S., Yeo S. S. & Kim S. K., Securing against brute-force attack: A Hash-based RFID mutual authentication protocol using a secret value, Computer Communications, 34(3), 2011.

[6] Moosavi, S.R.; Nigussie, E.; Virtanen, S.; Isoaho, J. An elliptic curve-based mutual authentication scheme for RFID implant systems. Procedia Comput. Sci. 2014, 32, 198–206.

[7] Farash M.S.”Cryptoanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography”. The Journal of Supercomputing.Springer-US.2014.

[8] He, D.; Kumar, N.; Chilamkurti, N.; Lee, J.H. Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. J. Med. Syst. 2014, 38, 1–6.

[9] Z. Liu, D. Liu, L. Li, H. Lin and Z. Yong, Implementation of a New RFID Authentication Protocol for EPC Gen2 Standard, IEEE Sensors Journal, Vol. 15, No. 2, Fenruary 2015

[10] Khatwani, C.; Roy, S. Security Analysis of ECC Based Authentication Protocols. In Proceedings of the 2015 International Conference on Computational Intelligence and Communication Networks (CICN), Jabalpur, India, 12–14 December 2015; pp. 1167–1172.

[11] D. Liu, Z. Liu, Z. Yong, X. Zou and J. Cheng, Design and Implementation of an ECC-Based Digital Baseband Controller for RFID Tag Chip, IEEE Transactions on Industrial Electronics, Vol. 62, No. 7, July 2015

[12] Mustapha Benssalah and Mustapha Djeddou, Design and Implementation of a New Active RFID Authentication Protocol Based on Elliptic Curve Encryption, SAI Computing Conference 2016 July 115, 2016 | London, UK

[13] Chuang, Y.H.; Hsu, C.L.; Shu, W.; Hsu, K.C.; Liao, M.W. A Secure Non-interactive Deniable Authentication Protocol with Certificates Based on Elliptic Curve Cryptography. In New Trends in Intelligent information and Database Systems; Springer: Berlin, Germany, 2015; pp. 183–190.

[14] Jin, C.; Xu, C.; Zhang, X.; Zhao, J. A secure RFID mutual authentication protocol for healthcare environments using elliptic curve cryptography. J. Med. Syst. 2015, 39, 1–8.

[15] .47 Ye, N.; Zhu, Y.; Wang, R.C.; Malekian, R.; Min, L.Q. An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things. Int. J. Appl. Math. Inf. Sci. 2014, 8, 1617–1624.

[16] Mahalle, P.N.; Prasad, N.R.; Prasad, R. Object Classification based Context Management for Identity Management in Internet of Things. Int. J. Comput. Appl. 2013, 63, 1–6

[17] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, pp. 2266-2279, 2013.

[18] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, "On the Security and Privacy of Internet of Things Architectures and Systems," in International Workshop on Secure Interner of Things (SIOT) 2015.

[19] P. Gope and T. Hwang, "A Realistic Lightweight Authentication Protocol Preserving Strong Anonymity for Securing RFID System," Computers & Security, vol. 55, pp. 271–280, 2015.

[20] P. Gope and T. Hwang, "Enhanced Secure Mutual Authentication and Key Agreement Scheme Preserving User Anonymity in Global Mobile Networks," Wireless Personal Communications, vol. 82, pp. 2231-2245, 2015.

[21] Yaman Sharaf-Dabbagh, on the authentication of devices in the Internet of things, World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2016 IEEE 17th International Symposium on A

[22] Moreno Ambrosin , Arman Anzanpour , Mauro Conti , Tooska Dargahi, On the Feasibility of Attribute-Based Encryption on Internet of Things Devices, IEEE Micro Special Issue on Internet of Things (2016).

[23] Suyel Namasudra, Pinki Roy, An improved attribute-based encryption technique towards the data security in cloud computing, 2017.