نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال یازدهم، شماره ۴، زمستان ۱۳۹۹؛ ص ۴۵۰-۴۳۹

«علمی- پژوهش»

بهبود احراز هویت در خانه هوشمند مبتنی بر رمز یکبار مصرف و رمزنگاری منحنی بیضوی

نرگس اسدنجفی[۱]، مهدی ملامطلبی[۲*]

۱- کارشناسی ارشد، ۲-استادیار، گروه کامپیوتر، واحد بوئین زهرا، دانشگاه آزاد اسلامی، بوئین زهرا، ایران

(دریافت: ۹۸/۰۷/۰۴، پذیرش: ۹۸/۱۲/۰۹)

چکیده

در خانه‌های هوشمند، اغلب اشیا با یکدیگر و با افراد خانه، در تعامل هستند. یکی از مزایای خانه هوشمند، امکان کنترل و نظارت بر خانه، از راه دور است. درعین‌حال، خانه هوشمند به‌طور بالقوه در معرض مشکلات امنیتی و نقض حریم خصوصی افراد است. با توجه به این‌که اشیاء درون خانه هوشمند، همواره در حال جمع‌آوری اطلاعات خصوصی از فعالیت‌های افراد هستند، اگر شخصی به اشیاء داخل منزل، به‌طور غیرمجاز دسترسی یابد، اشیا را تحت کنترل خود درآورده و به داده‌های خصوصی افراد دست‌یافته و باعث صدمه زدن به اشیا و یا فاش نمودن اطلاعات می‌نماید. جهت جلوگیری از این امر، افرادی که قصد استفاده از اشیاء داخل منزل را دارند، باید پیش از استفاده، احراز هویت گردند. در این مقاله، روشی برای بهبود احراز هویت افراد، مبتنی بر رمز یکبار مصرف با استفاده از کارت هوشمند و الگوریتم رمزنگاری منحنی بیضوی در سامانه خانه هوشمند، ارائه‌شده است. ارزیابی روش پیشنهادی توسط منطق بن و در محیط نرم‌افزار آویسپا انجام شده است. نتایج ارزیابی‌ها حاکی از بهبود احراز هویت متقابل بین کاربر و گره دروازه جهت مقابله با حملات متداول به خانه هوشمند، در مقایسه با روش‌های موجود است. به‌علاوه، روش پیشنهادی از حملات استراق سمع و حمله سرک‌کشی جلوگیری می‌نماید که اکثر روش‌های موجود، قادر به جلوگیری از آنها نیستند.

کلیدواژه‌ها: احراز هویت، خانه هوشمند، رمز یکبار مصرف، کارت هوشمند، رمزنگاری منحنی بیضوی.

Improving the Authentication in Smart Home Using One-Time Password and Elliptic-Curve Cryptography

N. Asadnajafi, M. Mollamotalebi*
Department of Computer, Buinzahra Branch, Islamic Azad University, Buinzahra, Iran
(Received: 26/09/2019; Accepted: 28/02/2020)

Abstract

In smart homes, most objects interact with each other and with people in the home. One of the advantages of a smart home is the ability to control and monitor the home remotely. At the same time, the smart home is potentially vulnerable to security issues and privacy violance. Given that objects inside the smart home are always collecting private information about people's activities, if someone unauthorizedly accesses objects inside the house, they take control of the objects and give them data. Private property is accessed by individuals and causes damage to objects or disclosure of information. To prevent this, people who intend to use indoor objects must be authenticated before use. In this paper, a method to improve the authentication of individuals, based on one-time password using a smart card and elliptic curve encryption algorithm in the smart home system, is presented. The evaluation of the proposed method is done by Ban Logic and in Avispa environment. The results of the evaluations indicate an improvement in the mutual authentication between the user and the gateway node to deal with common attacks on the smart home, compared to existing methods. In addition, the proposed method prevents eavesdropping attacks and Shoulder surfing attacks that most existing methods are unable to prevent.

Keywords: Authentication, Smart Home, One-Time Password, Smart Card, Elliptic-Curve Cryptography.

*Corresponding Author E-mail: motalebi@qiau.ac.ir

۱. مقدمه

در دنیای مدرن امروز، با پیشرفت علم و فناوری، اشیا هوشمند به‌طور تقریباً نامحسوسی وارد جریان زندگی روزمره افراد شده‌اند. این اشیا می‌توانند پوشیدنی و یا خوردنی بوده و یا از اجزا تشکیل‌دهنده خانه باشند. یک خانه با قطعات هوشمند مرتبط باهم، ممکن است حاوی داده‌های بااهمیتی (نظیر تصاویر و ویدئوهای شخصی که به‌صورت دیجیتالی نگهداری می‌شوند) باشد.

دستگاه‌هایی مانند دوربین‌های باقابلیت اتصال به شبکه که از راه دور کنترل می‌شوند، میکروفون‌های نصب‌شده در منزل که صحبت‌های محرمانه را شنود می‌کنند و بسیاری تجهیزات دیگر، امروزه حریم خصوصی و امنیت افراد را به مخاطره می‌اندازند [۱]. مثلاً، سامانه‌های سخن گوی هوشمند[1] مانند محصول اکو[2] ساخت شرکت آمازون و میکروفون خانگی شرکت گوگل که برنامه‌ریزی‌شده‌اند تا دستور "بیدار شو" را اجرا کنند و بعداز آن دستور، دستوراتی که به‌وسیله صدا به آن‌ها داده می‌شود (کارهایی مثل کم کردن نور یا پخش موسیقی) را می‌شنوند و اجرا می‌کنند [۲]. در بسیاری از موارد، معضلات امنیتی شبکه‌های بی‌سیم یا اقتضایی، به خانه‌های هوشمند نیز تسری می‌یابند [۳].

لذا اشیا هوشمند، اطلاعات گاه ارزشمند و محرمانه‌ای را که مربوط به اعضای خانه (کاربران) است دربردارند که بایستی از دسترسی غیرمجاز، محافظت گردند. ازاین‌رو، موضوع احراز هویت افرادی که مجاز به استفاده از اشیا خانه هوشمند هستند، بحثی حیاتی محسوب می‌شود. صرفاً افراد مجاز می‌توانند قابلیت دسترسی، برنامه‌ریزی و یا فرماندهی به اشیا هوشمند را داشته باشند و دسترسی افراد خرابکار[3] به این اشیاء بایستی مسدود باشد تا از خسارات مالی و گاهی جانی افراد جلوگیری نمود [۴] [۵].

روش‌های مختلفی جهت مقابله با تهدیدهای احراز هویت کاربران خانه هوشمند ارائه‌شده‌اند که هرکدام مزایا و معایبی دارند. با درنظر گرفتن متحرک بودن کاربران و اجازه دسترسی و ورود از مکان‌های مختلف، روش‌های احراز هویت رایج، مانند استفاده از نام کاربری و رمز عبور، به‌تنهایی، ناکارآمد بوده و نیاز به بهبود روش‌های احراز هویت، مشهود است.

در معماری و طراحی‌های فعلی خانه‌های هوشمند، توجه چندانی به مساله امنیت و حریم خصوصی افراد نشده است و درنتیجه، در یک خانه هوشمند با قدرت امنیتی پایین، اطلاعات محرمانه کاربران به راحتی در اختیار افراد ناشناس یا مخرب قرار می‌گیرد [۶]. از طرفی نیز، با توجه به ویژگی ارتباط چند پروتکلی و قابلیت‌های متنوع دستگاه‌ها، راهکارهای امنیتی سنتی برای قطعات خانه هوشمند، کارایی مناسبی ندارند [۲]. روش امنیتی که در خانه‌های هوشمند ارائه می‌شود باید سازگاری بین استانداردهای چندگانه را نیز در نظر داشته باشد.

احراز هویت باید یک روال کلی باشد به این معنی که، کاربر برای دسترسی به سامانه و تک‌تک ابزارهای وابسته به آن، فقط یک‌بار احراز هویت شود، و برای استفاده از هر یک از دستگاه‌های موجود در سامانه، نیازی به احراز هویت مجدد نداشته باشد. علاوه بر آن، این روال باید امنیت سامانه را بالا برده و استفاده از رابط کاربری را به حداقل برساند و همچنین از روش‌های احراز هویت بیومتریک به‌دلیل هزینه‌بر بودن آن‌ها، ترجیحاً استفاده نکند. با توجه به عامل‌ها و نیازهای عنوان‌شده و تحقیقاتی که پیش‌ازاین صورت گرفته است، می‌توان ادعا کرد که استفاده از روش احراز هویت مبتنی بر رمز یکبار مصرف با استفاده از کارت هوشمند و الگوریتم منحنی بیضوی در سامانه خانه هوشمند در تحقیق حاضر، توجیه‌پذیر است.

این مقاله در ادامه، شامل بخش‌های زیر است. بخش دوم به مرور روش‌های مرتبط و نقد و بررسی آن‌ها می‌پردازد. روش پیشنهادی این مقاله در بخش سوم با جزئیات تشریح شده است. در بخش چهارم، نتایج روش پیشنهادی این تحقیق با روش‌های مرتبط اخیر، مقایسه و ارزیابی می‌گردد و بخش پنجم به نتیجه‌گیری این مقاله می‌پردازد.

۲. کارهای مرتبط

اشیا هوشمند موجود در یک خانه هوشمند، با پروتکل‌های مختلفی مانند زیگبی[4]، زِد- ویو[5]، کِی‌اِن‌ایکس[6]، تِرِد[7]، و اِس‌سی‌اس[8] و شیوه‌های ارتباطی گوناگونی نظیر وای‌فای، بلوتوث، آراِف‌آیدی، و اِن‌اف‌سی[9]، با یکدیگر ارتباط برقرار می‌کنند [۷] و گاهی جهت ارتباط، نیازمند استفاده از پل[10]، هاب و دروازه[11] هستند. همچنین ممکن است یک دستگاه از پروتکل اختصاصی به‌منظور ارتباطات محلی (پروتکل بدون استفاده از IP) و از یک

[1] Smart speaker systems
[2] Echo
[3] Intruder

[4] Zig-bee
[5] Z-wave
[6] KNX
[7] Thread
[8] SCS
[9] NFC
[10] Bridge
[11] Gateway

پروتکل استاندارد، برای اتصال به ابر[1]، استفاده کند. این عوامل در کنار محدودیت‌های سخت‌افزاری، باعث شده روش‌های رمزنگاری ضعیفی در خانه‌های هوشمند به کار گرفته شوند [۲]. در ادامه، تحقیقات مرتبط با امنیت و احراز هویت در خانه‌های هوشمند، معرفی می‌شوند.

صالح اصفهانی و همکارانش [۳] یک چارچوب احراز هویت متن- آگاه[2] جهت حفاظت از دستگاه‌های هوشمند در برابر دسترسی‌های غیرمجاز ارائه داده است. در زمان ورود کاربر جدید به سامانه، اطلاعات کاربر، مانند مکان، پروفایل، تقویم برنامه‌ریزی، زمان درخواست و الگوهای رفتاری دسترسی وی، ثبت می‌شود و یک سطح دسترسی معین توسط صاحب‌خانه، برایش ثبت می‌شود. زمانی که کاربر نیاز به دسترسی به خانه هوشمند، از خارج آن داشته باشد، این اطلاعات جهت تصمیم‌گیری در خصوص پذیرش یا رد درخواست کاربر استفاده می‌شوند.

این چارچوب توانایی حفاظت از قطعات خانه هوشمند را در برابر دسترسی غیرمجاز کاربران محلی و راه دور دارد. همچنین بر دسترسی‌ها و فعالیت‌هایی مانند ورود کاربر، درخواست سرویس، و مدت زمان استفاده از خدمت نظارت دارد و این اطلاعات را، در یک پایگاه داده جهت استفاده در آینده، ثبت می‌نماید و می‌تواند جهت مقابله با حمله بروت‌فورس[3] نیز مفید واقع شود. از سوی دیگر، این چارچوب در برابر حمله سرک‌کشی آسیب‌پذیر است به‌طوری‌که اگر شخصی با سرک‌کشیدن، اطلاعات کاربر را به‌دست آورد، به راحتی می‌تواند به‌جای او وارد سامانه شود.

در روش پیشنهادی سانتوس و همکارانش [۴]، احراز هویت کاربران توسط گوشی‌های هوشمند مجهز به صفحه لمسی صورت می‌گیرد. تعداد ۳۰ الگوی رفتاری لمس کردن صفحه گوشی هوشمند توسط کاربر (مثلاً حرکت به راست و چپ یا بالا و پایین) ثبت می‌شود و با بررسی تعاملات کاربر حاضر با صفحه لمسی، نشست کاری وی، حفظ یا حذف می‌گردد. این چارچوب در مقابل حمله سرک‌کشی و جعل هویت کاربر، مقاوم است ولی نمی‌تواند به‌عنوان یک روش مستقل احراز هویت، استفاده شود؛ بلکه باید به‌عنوان بخشی از سامانه احراز هویت چندحالته[4] استفاده شود. همچنین در این چارچوب، همه دستگاه‌های مورد استفاده کاربر، باید مجهز به صفحه لمسی باشند و ممکن است کاربر در استفاده از آن، راحت نباشد و یا متحمل هزینه بیشتر گردد.

جیونگ و همکارانش [۸] روشی جهت احراز هویت با استفاده از رمز یکبار مصرف و کارت هوشمند در شبکه خانه هوشمند، ارائه داده است. این روش به‌دلیل استفاده از تابع چکیده‌سازی یک‌طرفه، بار محاسباتی کمی دارد هرچند که احراز هویت متقابل بین گره دروازه و قطعات هوشمند، کاربر و قطعات هوشمند را ارائه نمی‌دهد. پیام‌ها در آن می‌توانند ردیابی شوند و برای کاربر دور از خانه، مناسب نیست. کاستی دیگر این روش، ناامن بودن در برابر حمله سرک‌کشی و دزدیده شدن کارت هوشمند است. مهاجم می‌تواند بعد از به دست آوردن کارت، به تمام اطلاعات محرمانه کاربر که در آن ذخیره‌شده است، دسترسی یابد. روش ارائه‌شده توسط وایدیا و همکارانش [۹] که در آن، احراز هویت کاربران بر اساس کلمه عبور است نیز، از مشکلات مشابه رنج می‌برد.

سانتوسو و همکارانش [۱۰] روشی مبتنی بر رمزنگاری منحنی بیضوی جهت احراز هویت، ارائه داده است. هویت کاربر توسط دستگاه‌هایی که داخل خانه هوشمند قرار دارند و با یک گره مرکزی دروازه مرتبط هستند، محرز می‌شود. این روش در ناشناس نگاه‌داشتن دستگاه‌ها و به‌تبع آن، کاربر، ناتوان است.

چنگ و همکارانش [۱۱] یک روش احراز هویت دو عاملی برای شبکه‌های حسگر بی سیم با استفاده از کارت هوشمند و رمز عبور ارائه کرده است. در آن، از دو پروتکل استفاده‌شده است؛ پروتکل اول بر اساس تابع چکیده‌سازی و عملگر بیتی یای انحصاری، و پروتکل دوم بر اساس تابع چکیده‌سازی و رمزنگاری منحنی بیضوی و عملگر بیتی یای انحصاری کار می‌کند. این روش، احراز هویت متقابل را تأمین می‌کند ولی در برابر حمله تکرار[5] و حمله فرد میانی[6] مقاوم نیست. پروتکل اول در برابر حمله قفل و کلید در نشست‌ها ناامن است و هر دو پروتکل در برابر حمله حدس رمز عبور، ناامن هستند. جهت از میان بردن محدودیت های این دو پروتکل، روش احراز هویت دیگری توسط داس و همکارانش[۱۲] ارائه‌شده است که از کلید و رمزنگاری منحنی بیضوی استفاده می‌کند هرچند که هیچ تمهیدی برای حمله سرک‌کشی ارائه نمی‌دهد.

وزید و همکارانش [۱۳] یک روش احراز هویت متقابل از راه دور و برقراری ارتباط با کلید ارائه داده است. این روش، احراز هویت متقابل بین کاربر و گره دروازه، اشیا و گره دروازه، و کاربر و

[1] Cloud
[2] Context-aware authentication framework
[3] Brute force
[4] Multi-modal
[5] Replay
[6] Man in the middle

اشیا را اداره می‌کند. نتایج بررسی امنیت این روش با استفاده از ابزار آویسپا و شبیه‌ساز NS2، نشان می‌دهد که در حفظ امنیت خانه هوشمند در برابر حملات متداول، امن است. بااین‌حال، در برابر حمله سرک‌کشی ضعیف است.

کومار و همکارانش [۱۴] روشی بر پایه کلید امن برای خانه هوشمند ارائه داده است. برای ایجاد اعتماد متقابل، واحد کنترل هر دستگاه هوشمند، با استفاده از توکن‌های احراز هویت، یک نشست کلید با گره دروازه برقرار می‌کند. گره دروازه ناشناس نیست و احراز هویت متقابل بین کاربر و قطعات هوشمند، و کاربر و گره دروازه را تأمین نمی‌کند. لی و همکارانش [۱۵] یک روش مبتنی بر رمزنگاری منحنی بیضوی در سامانه مدیریت انرژی خانه هوشمند، معرفی نموده است که ازنظر زمان و حافظه مصرفی، کارایی مناسبی دارد هرچند که برای حمله سرک‌کشی در آن، تدبیری اندیشیده نشده است.

نوی و همکارانش [۱۸] برای جلوگیری از دسترسی غیرقانونی افراد به داده‌های تولید شده توسط اشیا هوشمند، روش کم مصرف[1] احراز هویت بر مبنای پسورد را ارائه نمودند. در این روش امنیت خانه هوشمند بهبود یافته است و میزان مصرف انرژی دستگاه‌های هوشمند کاهش پیدا کرده است اما برای مقابله با حمله سرک کشی راه حلی ارائه نشده است.

منگشیا شوای و همکارانش [۱۹] برای مقابله با دزدیده شدن اطلاعات از کانال‌های ارتباطی اشیا هوشمند روشی ارائه کرده‌اند. این روش برای مقابله با اکثر حملات احتمالی راه حل مناسبی است، اما برای حمله استراق سمع و حمله سرک کشی راه‌حلی ارائه نکرده است.

مهدی اکبری گورابی [۲۰] یک روش مبتنی بر سخت‌افزار با استفاده از کارت هوشمند و احراز هویت دوفاکتوره ارائه کرده است. این روش، رازداری پیش‌رو[2] را ارائه نمی‌دهد، حمله استراق سمع و سرک کشی را نیز بررسی نمی‌کند. اما در برابر حملات تکرار و یا دزدیده شدن کارت، مقاوم است.

با عنایت به موارد فوق، روش‌های موجود در تأمین احراز هویت ازنظر حملات متداول به خانه هوشمند، ضعف دارند. لذا در مقاله حاضر، یک روش مبتنی بر رمز یکبار مصرف و استفاده از کارت هوشمند و الگوریتم منحنی بیضوی، به‌منظور بهبود روش‌های پیشین، و مقابله با حملات متداول، ارائه‌شده است. در این روش، احراز هویت متقابل بین کاربر و گره دروازه و همچنین اشیا خانه هوشمند و گره دروازه، انجام می‌شود.

۳. روش پیشنهادی

روش پیشنهادشده در این مقاله، از دو بخش تشکیل‌شده است. بخش اول مربوط به احراز هویت فرد و سرویس‌دهنده خانه هوشمند است و شامل سه مرحله ثبت کاربر، ورود افراد/احراز هویت، و درخواست خدمت است. در مرحله ثبت کاربر، اطلاعات کاربر در سرویس‌دهنده ثبت می‌گردد. پس از ثبت اطلاعات، به او یک کارت هوشمند تعلق می‌گیرد. در مرحله ورود افراد/احراز هویت، کاربر کارت هوشمند را وارد پایانه می‌کند و باید اثبات شود که او همان شخصی است که قبلاً در سرویس‌دهنده خانه هوشمند ثبت‌شده بود. پس از احراز هویت کاربر توسط سرویس‌دهنده، کاربر درخواست استفاده از هریک از لوازم هوشمند موردنظرموردنظرش را به گره دروازه موجود در خانه هوشمند، ارسال می‌کند.

در بخش دوم، گره دروازه درخواست کاربر را دریافت کرده است و کاربر باید برای استفاده از وسیله هوشمند موردنظرموردنظرش، توسط گره دروازه، احراز هویت گردد. پس از احراز هویت دوطرفه بین کاربر و گره دروازه و مجاز شناخته شدن کاربر، درخواست استفاده از شی هوشمند توسط گره دروازه، برای شی موردنظر ارسال می‌گردد. در این مرحله، یک احراز هویت دوطرفه نیز بین گره دروازه و شی هوشمند انجام می‌گیرد تا گره دروازه از مخرب نبودن شی هوشمند مطمئن شود و شی هوشمند نیز از این‌که درخواست از طرف گره دروازه برای او ارسال‌شده است، اطمینان یابد. برای توضیح و تفسیر مراحل روش پیشنهادی، در این تحقیق از یک سری علائم اختصاری استفاده‌شده که در جدول (۱) نشان داده شده‌اند.

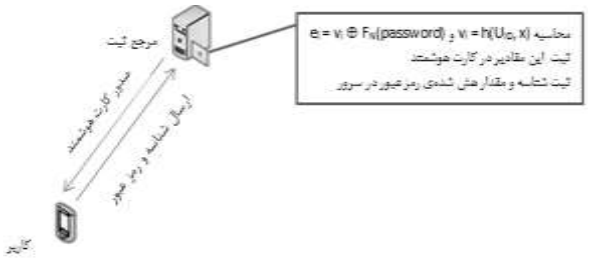
جدول ۱. علائم اختصاری استفاده‌شده در روش پیشنهادی

علامت	توضیح
RA	مرجع ثبت
R_{Ui}	عدد حاصل از چکیده‌سازی رمز کاربر در RA
R_{Si}	عدد تصادفی تولیدشده توسط RA
F(), h()	توابع چکیده‌سازی
N	تعداد دفعات مجاز ورود در مدت زمان معتبر بودن بلیط
S_{key}	کلید مشترک بین دروازه و کاربر
U_{ID}	کاربر دارای شناسه کاربری
RA_{ID}	شناسه RA
$E_{RA-GW}()$	رمزگذاری با استفاده از کلید متقارن بین RAو GW
E_K	رمزگذاری با استفاده از K
E_K	مهرزمانی نشان‌دهنده معتبر بودن کلید نشست

[1] lightweight
[2] Forward secracy

لازم به توضیح است که دو پارامتر N و T برای محدود کردن کاربر استفاده می‌شوند. برای مثال، اگر N=150 و (ماه)T=1 باشد، یعنی یک کاربر مجاز، می‌تواند در طول یک ماه، ۱۵۰مرتبه، بدون ورود/ احراز هویت مجدد، به گره دروازه دسترسی داشته باشد. در ادامه، فازهای مختلف بخش اول روش پیشنهادی تشریح می‌شوند.

در مرحله ثبت کاربر، فرض می‌شود که x یک کلید سری است که در مرجع ثبت، نگهداری می‌شود. تابع h() به‌عنوان یک تابع چکیده‌ساز در نظر گرفته می‌شود. U نیز به‌عنوان کاربر در نظر گرفته می‌شود که درخواست احراز هویت می‌کند. همان‌گونه که در شکل (۱) نشان داده‌شده است، کاربر، شناسه و رمز خودش را جهت ثبت، به سامانه مرجع ثبت ارسال می‌کند. مرجع ثبت، بعد از دریافت شناسه و رمز از کاربر، عملیات زیر را اجرا می‌کند: ۱) عبارت‌های $v_i = h(U_{ID}, x)$ و $e_i = v_i \oplus F_N(password)$ را برای U محاسبه می‌کند و آن‌ها را به‌عنوان اطلاعات سری U در نظر می‌گیرد. ۲) مقدار v_i و e_i را در حافظه کارت هوشمند ثبت می‌کند و کارت را برای U صادر می‌کند و در اختیار او می‌گذارد. $F_N(0)$ مقدار نهایی چکیده‌سازی پذیرفته‌شده برای کاربر است. ۳) درنهایت، سرویس‌دهنده مقدار U_{ID} و رمزی را که توسط تابع F درهم شده است، در خودش نگه می‌دارد. این عملیات در مرحله ثبت هر کاربر جدید، به‌صورت مجزا برای هر کاربر اجرا می‌شود.



شکل ۱. مرحله ثبت کاربر در مرجع ثبت

در مرحله ورود و احراز هویت، وقتی کاربر U_{ID} قصد ورود به سامانه مرجع ثبت را داشته باشد، باید کارت هوشمند را در پایانه وارد کند و شناسه U_{ID} و رمز عبور $F_N(password)$ را وارد کند. سپس کارت هوشمند، عملیات زیر را اجرا می‌کند:

۱) برای i اُمین احراز هویت کاربر، به تعداد i مرتبه، تابع چکیده‌سازی $F^i_N(password)$ را اجرا می‌کند و نتیجه را محاسبه می‌کند.

۲) مقدار $C = h(e_i \oplus F^i_N(password))$ را محاسبه می‌کند.

۳) پیام محتوی (U_{ID}, C) را که درواقع، پیام درخواست احراز هویت است، به مرجع ثبت ارسال می‌کند. بعد از این‌که اطلاعات توسط سرویس‌دهنده مرجع ثبت دریافت شد، برای برقراری احراز هویت بین کاربر و مرجع ثبت، مراحل بعد در مرجع ثبت اجرا می‌شود.

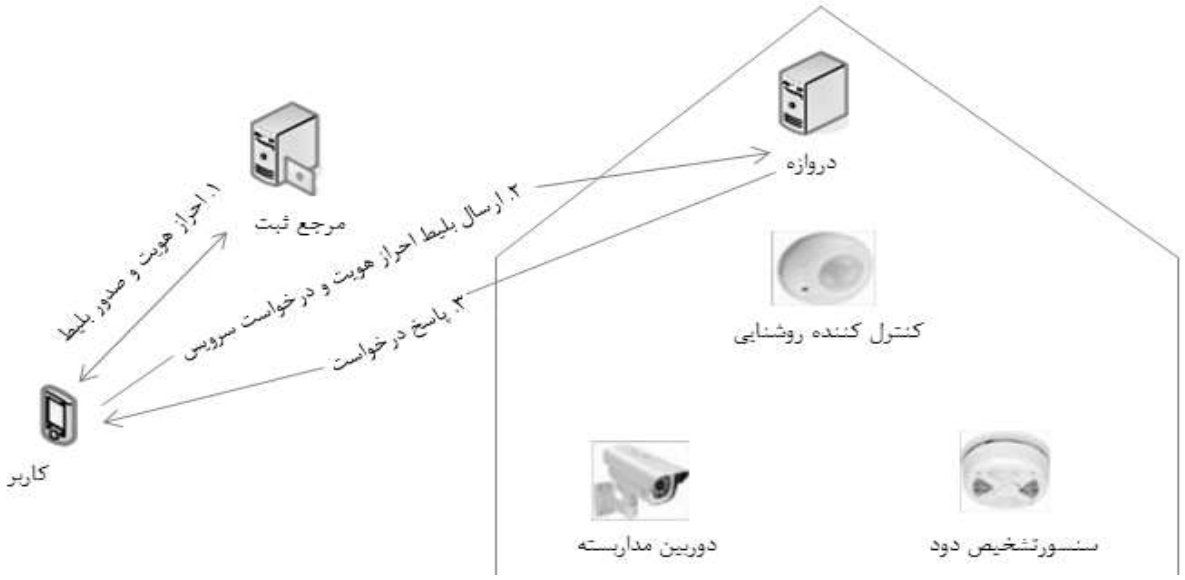
۴) سرویس‌دهنده، U_{ID} را می‌شناسد و تائید می‌کند. سپس یک مقدار $v'_i = h(U_{ID}, x)$ تولید می‌گردد و بررسی می‌شود که آیا $C = h(e'_i \oplus F'^i_N(password))$ است یا خیر. سپس به مقدار چکیده‌سازی کاربر و سرویس‌دهنده، یک واحد اضافه می‌شود، یعنی $F^i_N(password)$ برای کاربر و $F^{i+1}_N(password)$ برای سرویس‌دهنده. اگر این دو مقدار برابر نباشند، درخواست کاربر رد و در غیر این‌صورت، تائید می‌شود. در صورت تائید، سرویس‌دهنده باید اطلاعاتی را برای استفاده او از خانه هوشمند و ارتباط او با دروازه در اختیارش بگذارد.

۵) سرویس‌دهنده مقدار عدد تصادفی یکبار مصرف R_{Si} را تولید می‌کند و مقدار $F^i_N(password)$ را درون R_{Ui} قرار می‌دهد؛ سپس مقدار $S_{key} = h(R_{Si}, R_{Ui})$ را محاسبه می‌کند.

۶) سرویس‌دهنده یک بلیط احراز هویت تولید می‌کند و آن را با کلید متقارن که بین خودش و دروازه، مشترک است، قفل می‌کند. سپس $E_{RA-GW}(U_{ID}, RA_{ID}, R_{Ui}, R_{Si}, T)$ را به همراه پیامی که نشان‌دهنده این است که کاربر احراز هویت شده است به‌صورت $E_{RUi}(U_{ID}, RA_{ID}, R_{Ui}, R_{Si}, T, h(S_{key}, U_{ID}))$ به کاربر می‌فرستد.

۷) کاربر با دریافت پیام متوجه می‌شود که درخواست احراز هویت او پذیرفته‌شده است. حال باید مطمئن شود که پیام از سمت سرویس‌دهنده است. کاربر با دانستن $R_{Ui} = F^i_N(password)$ پیام را رمزگشایی می‌کند و با دست یافتن به R_{Si} از داخل پیام می‌تواند مقدار $S_{key} = h(R_{Si}, R_{Ui})$ را محاسبه کند و با دانستن S_{key}، مقدار $h(S_{key}, U_{ID})$ را به دست آورده و با تابع $h(S_{key}, U_{ID})$ که از طرف سرویس‌دهنده فرستاده‌شده، مقایسه می‌کند و مطمئن می‌شود که پیام از سمت سرویس‌دهنده است.

قابل‌توجه است که فقط کاربرِ مجاز، مقدار password را می‌داند و به R_{Ui} دسترسی دارد؛ پس فقط کاربر مجاز می‌تواند پیامی که از سمت سرویس‌دهنده آمده است را رمزگشایی کند و R_{Si} را به‌دست آورد. برای ساده‌سازی و درک سازوکار احراز هویت کاربر، به شکل (۲) توجه شود.

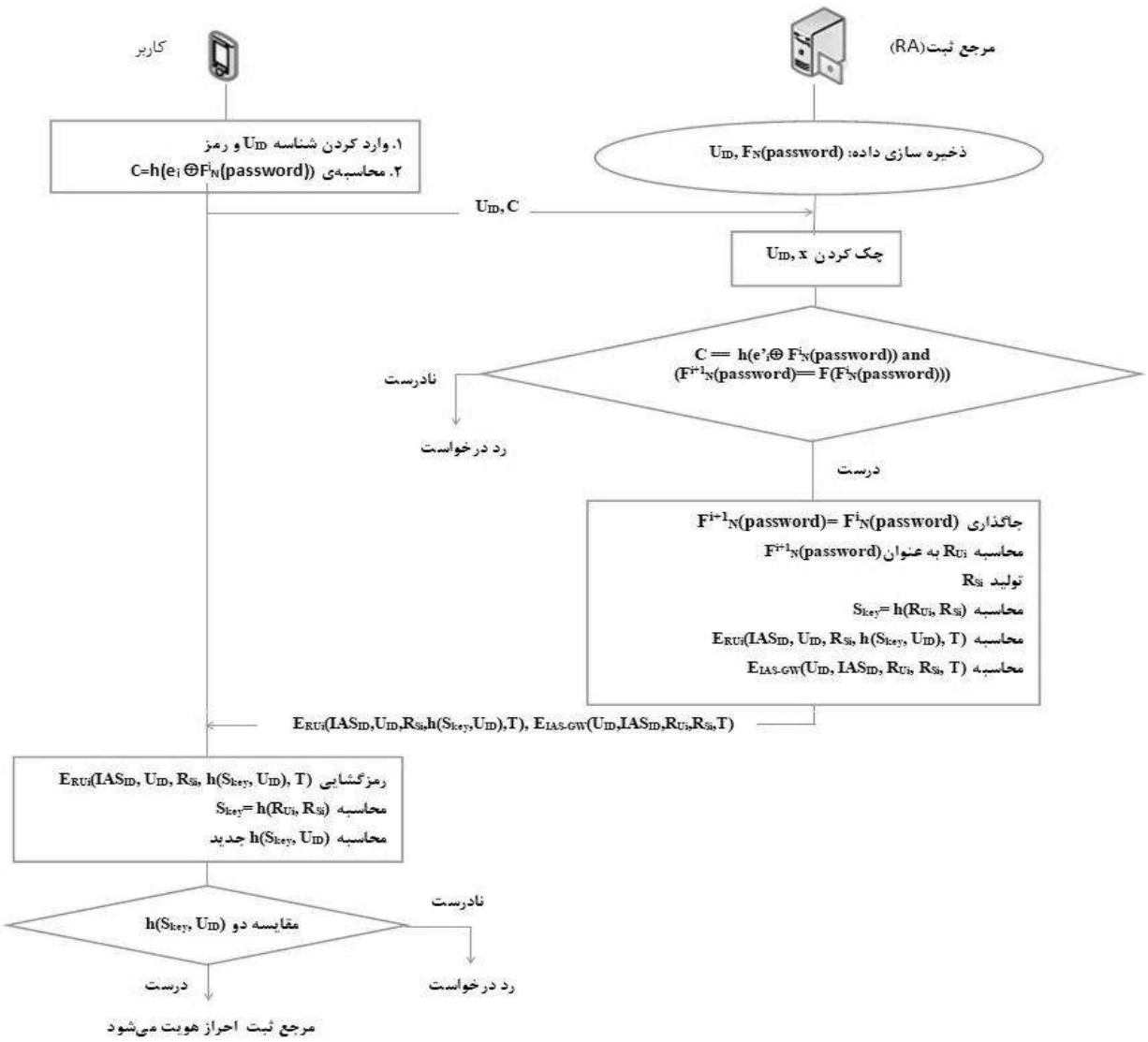


شکل ۲. سازوکار احراز هویت کاربر

با توجه به شکل (۲)، در روش پیشنهادی، یک مرجع ثبت، چند شی هوشمند، یک گره دروازه و کاربرانی که قصد دسترسی به خانه را دارند، در نظر گرفته می‌شوند. قبل از همه، ثبت هر دستگاه هوشمند و گره دروازه در مرجع ثبت (RA)، انجام‌شده است. اگر کاربری بخواهد به دستگاه‌های هوشمند دسترسی داشته باشد و از خدمات خانه هوشمند استفاده نماید، باید از طریق مرجع ثبت، احراز هویت شود و بلیط احراز هویت را دریافت کند. این بلیط برای ارتباط کاربر با گره دروازه، کاربرد دارد. کاربری که احراز هویت شده است، برای استفاده از خدمات خانه هوشمند، به این بلیط نیاز دارد.

در شکل (۳)، مرحله ورود و احراز هویت نشان داده‌شده است. یک درخواست احراز هویت از سوی کاربر به سرویس‌دهنده ارسال می‌شود و بعد از تائید اطلاعات کاربر از سوی سرویس‌دهنده، یک پاسخ از سمت سرویس‌دهنده برای کاربر ارسال می‌شود. کاربر نیاز دارد که پاسخ دریافت شده از سمت سرویس‌دهنده را تائید اعتبار نماید. در مرحله درخواست سرویس، بعد از این‌که کاربر، توسط مرجع ثبت، تائید و احراز هویت گردید، به‌عنوان کاربر مجاز شناخته می‌شود؛ یعنی این کاربر اجازه دارد تا از خدمات خانه هوشمند استفاده کند. برای این کار، کاربر باید درخواست خود را به‌صورت$(U_{ID}, \text{Service})$ که شامل شناسه او و خدمت درخواستی است، به سمت گره دروازه ارسال کند. این درخواست به‌وسیله S_{key} رمزگذاری شده و از سوی کاربر به همراه بلیطی که کاربر در مرحله قبل، از سرویس‌دهنده دریافت کرده، یعنی $E_{RA-GW}(U_{ID}, RA_{ID}, R_{Ui}, R_{Si}, T)$، برای دروازه ارسال می‌شود.

در مرحله درخواست خدمت از سوی کاربر به سمت دروازه، دروازه دو پیام دریافت می‌کند. یک پیام، بلیطی است که سرویس‌دهنده از طریق کاربر برای او فرستاده است و دیگری، درخواست استفاده از خدمات خانه که توسط کاربر برای دروازه ارسال‌شده است. دروازه در ابتدا پیامی را که با کلید مشترک بین خودش و سرویس‌دهنده رمزگذاری شده بود، باز می‌کند. T را چک می‌کند و مطمئن می‌شود پیام معتبر است. با به دست آوردن R_{Ui} و R_{Si} از داخل بلیط دریافت شده، مقدار S_{key} را دست می‌آورد و با آن، پیام کاربر را رمزگشایی می‌کند. U_{ID} که در پیام کاربر است را با U_{ID} ای که توسط بلیط فرستاده شده است، مقایسه می‌کند و اعتبار کاربر را تائید می‌کند و به او اجازه دسترسی به خدمات خانه را می‌دهد. سپس R_{Ui} را با S_{key} رمزگذاری می‌کند و برای کاربر می‌فرستد و کاربر مطمئن می‌شود که پیامش به شخص مطمئن یا همان دروازه رسیده است و اعتبار دروازه هم نزد کاربر تائید می‌شود. بدین ترتیب، یک احراز هویت دوطرفه انجام می‌شود.



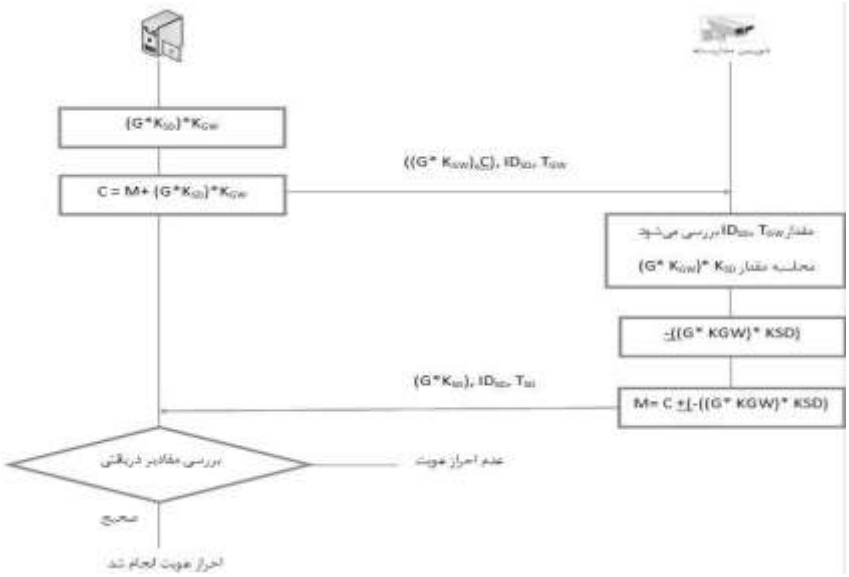
شکل ۳. مرحله ورود و احراز هویت کاربر i اُم

احراز هویت بین گره دروازه و دستگاه‌های خانه هوشمند بدین‌صورت است که ابتدا، تمام دستگاه‌های خانه هوشمند باید در مرجع ثبت RA ثبت شوند و یک شناسه یکتا دریافت کنند. پس‌ازآن برای استفاده از هر دستگاه، آن دستگاه توسط گره دروازه احراز هویت می‌گردد و آماده دریافت دستورات اجرایی می‌شود. مراحل ثبت و احراز هویت دستگاه‌ها به ترتیب، در ادامه ذکر می‌شوند:

۱) در مرحله ثبت دستگاه‌ها که توسط مرجع ثبت انجام می‌شود، برای هر دستگاه SD، یک شناسه یکتای ID_{SD} توسط مرجع ثبت درنظر گرفته می‌شود. علاوه بر آن، یک کلید خصوصی به نام K_{SD} و یک کلید عمومی $K_{SD}*G$ تولید می‌شود. این اطلاعات در پایان مرحله ثبت، در حافظه دستگاه SD ذخیره می‌شود. گره دروازه نیز مجهز به اطلاعات کلید خصوصی K_{GW} و کلید عمومی $K_{GW}*G$، و شناسه هر دستگاه هوشمند ID_{SD} می‌شود.

۲) در مرحله احراز هویت بین دستگاه‌ها و گره دروازه، کاربر درخواست استفاده از دستگاه را به‌صورت $(U_{ID}, Service)$ و $E_{RA-GW}(U_{ID}, RA_{ID}, R_{Ui}, R_{Si}, T)$ به گره دروازه ارسال می‌کند. پس از برقراری ارتباط و احراز هویت طرفین، گره دروازه درخواست را با استفاده از الگوریتم منحنی بیضوی، با توجه به مزیت طول کوتاه کلید در آن [۱۷]، رمزنگاری کرده و به همراه یک مهر زمانی T_{GW} و شناسه دستگاه موردنظر ID_{SD}، برای دستگاهی که خدمت آن درخواست شده است، ارسال می‌کند.

گره دروازه برای فرستادن پیام M به‌صورت رمزشده به دوربین مداربسته، ابتدا با حاصل‌ضرب کلید عمومی دستگاه هوشمند در کلید خصوصی خودش و حاصل‌جمع این مقدار با پیام اصلی، یک متن رمزی می‌سازد و آن را به همراه یک سری اطلاعات دیگر که در همین بخش به آن اشاره گردید، برای دستگاه موردنظر، ارسال می‌نماید. دستگاه پس از دریافت متن رمز شده، ابتدا شناسه خودش و مقدار مهر زمانی را چک می‌کند.



شکل ۴. مرحله احراز هویت بین دستگاه‌ها و گره دروازه

سپس با کلید خصوصی خودش، بخشی از پیامی که دریافت کرده بود را باز می‌کند و درنهایت، مقدار پیام را می‌یابد. دستگاه به‌منظور انجام احراز هویت دوطرفه، یک مهرزمانی، شناسه خودش و کلید عمومی کلید دروازه را برای آن ارسال می‌کند. گره، این مقادیر را دریافت می‌کند. اگر این مقادیر صحیح باشند، مشکلی در احراز هویت وجود نخواهد داشت ولی اگر تشخیص دهد که اطلاعات دریافتی نادرست بوده است، دستگاه احراز هویت نمی‌شود.

۴. ارزیابی روش پیشنهادی

روش پیشنهادی ابتدا با استفاده از منطق بن که یکی از روش‌های متداول ارزیابی عملکرد احراز هویت است، مورد ارزیابی قرارگرفته است. هر سه مرحله ثبت، ورود/ احراز هویت و درخواست خدمت با استفاده از منطق بن ارزیابی می‌شوند.

برخی از علائم اختصاری که در این بخش استفاده می‌گردند، قبلاً در جدول (۱) معرفی‌شده‌اند و علائم دیگری نیز در این بخش، معرفی خواهند شد. ابتدا پیام‌های ردوبدل شده بین طرفین در روش پیشنهادی باید به فرمول تبدیل شوند، اهداف مشخص شوند و سپس باید با استفاده از قوانین منطق بن، این اهداف اثبات شوند. در شکل (۴)، پیام‌ها و طرفینی که در روش پیشنهادی مورد استفاده قرار گرفته‌اند، مشخص شده مشخص شده‌اند. برای ارزیابی به‌وسیله منطق بن، کافی است همین پیام‌ها و طرفین، ایده‌آل‌سازی شوند و اهداف مشخص گردند و اثبات گردند.

۴-۱. ارزیابی با روش بن

الف- مرحله عمومی

باروز، عبدی و نیدهام، یک منطق احراز هویت را توصیف می‌کنند که در مقاله [۱۶] به‌اختصار به نام منطق بن شناخته می‌شود. سه مرحله اصلی برای تجزیه‌وتحلیل یک پروتکل با استفاده از منطق بن وجود دارد :

مرحله اول،بیان فرض‌ها و هدف‌ها به شکل فرمول است (مرحله وضعیت)،منطق از یک وضعیت شناخته‌شده به سمت وضعیتی می‌رود که به اهداف مسئله دست‌یابیم. مرحله دوم،تغییر شکل دادن پروتکل به فرمول است و در مرحله سوم، یک مجموعه از قوانین استنتاجی که شرایط اساسی نامیده می‌شود به دست می‌آید. شرایط اساسی از فرض‌ها شروع می‌شود و توسط فرمول‌ها به اهداف می‌رسد و زمانی که شرایط به اهداف می‌رسند یعنی فرض اثبات‌شده است و روش پیشنهادی درست کار می‌کند.

با توجه به توضیحاتی که ارائه گردید، در ابتدا پیام‌های ردوبدل شده بین طرفین در روش پیشنهادی باید به فرمول

تبدیل شوند، اهداف مشخص شوند و سپس باید با استفاده از قوانین منطق بن، این اهداف اثبات شود.برای ارزیابی به‌وسیله منطق بن، کافی است همین پیام‌ها و طرفین ایده‌آل‌سازی شوند و اهداف مشخص گردند و اثبات گردند.

بنابراین، ابتدا پیام‌هایی که بین طرفین روش پیشنهادی ردوبدل می‌گردد، به شکل زیر نمایش داده می‌شود:

Message 1: $U\rightarrow RA : U_{ID}, C$

این پیام به این معنی است که، کاربر، یک پیام برای مرجع ثبت فرستاده است که این پیام شامل کدکاربر و متن رمزشده c است.

Message 2: $RA\rightarrow U:\{U_{ID}, RA_{ID}, R_{Ui}, R_{Si}, T_{RA}\}K_{RA\text{-}GW}, \{RA_{ID}, U_{ID}, R_{Si}, h(S_{Key},U_{ID}), T_{RA}\}R_{Uis}$

مفهوم این پیام آن است که مرجع ثبت، پیامی برای کاربر فرستاده است که شامل دو بخش است. بخش اول پیامی است که به‌وسیله کلیدی که بین خودش و گره دروازه مشترک است، رمزگذاری شده است و بخش دوم، پیام مربوط به خود کاربر است و با کلید خصوصی کاربر، رمز شده است.

Message 3: $U\rightarrow GW: \{U_{ID}, RA_{ID}, R_{Ui}, R_{Si}, T_{RA}\} K_{RA\text{-}GW}, \{U_{ID}, Service, T_U\} S_{Key}$

فرم عمومی این پیام به این صورت است که کاربر یک پیام برای گره دروازه ارسال می‌کند؛ این پیام شامل دو بخش است. بخش اول، بخشی از پیامی است که در مرحله قبل، مرجع ثبت برای کاربر ارسال کرده بود و بخش دوم، محتوی درخواست خدمت کاربر و شناسه کاربر است.

Message 4: $GW\rightarrow U: \{T_{U+1}, R_{Ui}\} S_{Key}$

در این فرم عمومی، یک پیام از طرف گره دروازه برای کاربر ارسال‌شده است که حاوی مدت زمان اعتبار پیام و رمز مربوط به کاربر است.

ب- هدف

برای اثبات این‌که روش پیشنهادی درست کار می‌کند و اثبات احراز هویت دوطرفه بین کاربر و گره دروازه و کاربر و مرجع ثبت، اهداف زیر تعریف می‌شوند: هدف ۱: $U|\equiv R_{Si}$ ، هدف ۲: $U|\equiv T_{U+1}$. هدف اول به این معنی است که اگر کاربر، R_{Si} را ببیند، یعنی از طرف مرجع ثبت مورد اعتماد، احراز هویت شده است. هدف دوم آن است که اگر کاربر در پیام دریافتی از طرف گره دروازه، مقدار T_{U+1} را دریافت کند، اجازه دارد از لوازمی که درخواست کرده بود استفاده کند و درواقع، توسط گره دروازه احراز هویت شود.

ج- ایده‌آل‌سازی

به‌منظور اعمال منطق بن، باید پیام‌های مرحله عمومی به پیام‌های ایده‌آل تبدیل شوند. برای این کار، شناسه‌ها و متن‌ها تغییر شکل پیدا می‌کنند و فرم ظاهری پیام‌های عمومی به‌صورت زیر تغییر شکل می‌یابد:

Message 1: $U\rightarrow RA: U_{ID}, C$

Message 2: $RA\rightarrow U: \{N_c, R_{Ui}, R_{Si}, T_{RA}\}K_{RA\text{-}GW}, \{N_d, R_{Si}, h(S_{Key},U_{ID}), T_{RA}\}R_{Ui}$

Message 3: $U\rightarrow GW: \{N_c, R_{Ui}, R_{Si}, T_{RA}\} K_{RA\text{-}GW}, \{N_e, T_U\} S_{Key}$

Message 4: $GW\rightarrow U: \{T_{U+1}, R_{Ui}\} S_{Key}$

روند اثبات در منطق بن به معنی از شرایط به هدف رسیدن است. در ابتدا، اگر کاربر (U) و گره دروازه (GW) و مرجع ثبت (RA) به ترتیب با پارامترهای A، B و S نشان داده شوند، فرض‌های اولیه به شکل زیر می‌شوند:

$A|\equiv A\leftrightarrow S,\ A|\equiv(S\Rightarrow A\leftrightarrow B),\ A|\equiv\#T_S,\ A|\equiv\#T_a,\ A|\equiv R_{Ui}$

$B|\equiv B\leftrightarrow S,\ B|\equiv(S\Rightarrow A\leftrightarrow B),\ B|\equiv\#T_S$

$S|\equiv A\leftrightarrow S,\ S|\equiv B\leftrightarrow S,\ S|\equiv(A\leftrightarrow B),\ S|\equiv\#R_{Si}$

اثبات هدف ۱. پس از این‌که پیام ۱ فرستاده می‌شود، A پیامی را دریافت می‌کند (پیام۲) که قادر است بخشی از آن را بفهمد:

$A \lhd \{N_c, R_{Ui}, R_{Si}, T_S\}K_{SB}, \{N_d, R_{Si}, h(S_{Key},A_{ID}), T_S\}K_{RUI}$

A پیامی را که از سمت S دریافت کرده است، باز می‌کند، بخشی از پیام را که با کلید مشترک S و B رمز شده است، به همراه یک پیام درخواست خدمت که خودش تولید می‌کند برای B می‌فرستد و بخش دیگر را که متوجه آن می‌شود، رمزگشایی کرده، و مقدار RSi را می‌بیند:

طبق فرض $A|\equiv R_{Ui}$

$A|\equiv S|\equiv\{N_c, R_{Ui}, R_{Si}, T_S\}K_{SB}, (N_d, R_{Si}, h(S_{Key},A_{ID}), T_S)$

پس بخشی که A می‌تواند بخواند به‌صورت زیر است

$A|\equiv S|\equiv(N_d, R_{Si}, h(S_{Key},A_{ID}), T_S)$

طبق فرض $S|\equiv\#R_{Si}$، و درنتیجه، هدف ۱ به اثبات رسیده است و خواهیم داشت:

$$A|\equiv\#R_{Si} \quad (1)$$

طبق فرض، با جاگذاری U به‌جای A خواهیم داشت: $\#R_{Si}$ $U|\equiv$ که یعنی کاربر احراز هویت شده است و مطمئن است که پیام را از مرجع ثبت دریافت کرده است. بعد از اثبات ۱ و با استفاده از فرض، می‌دانیم که اگر $A|\equiv R_{Ui}$ آنگاه:

$$A|\equiv S_{Key} \quad (2)$$

اثبات هدف ۲. پیام ۳ از طرف A برای B فرستاده می‌شود. B از پیام دریافت شده، می‌تواند آن بخشی را که از طرف S برایش ارسال‌شده است، ببیند. آن را با کلید مشترک BS رمزگشایی می‌کند. از داخل پیام رمزگشایی‌شده، مقدار R_{Si} و R_{Ui} را به دست می‌آورد و با استفاده از آن‌ها، مقدار S_{Key} را محاسبه

می‌کند:

$B \lhd \{N_c, R_{Ui}, R_{Si}, T_S\}\ K_{SB}, \{N_e, T_A\}\ S_{Key}$
$B|\equiv S|\equiv \{N_c, R_{Ui}, R_{Si}, T_S\}\ K_{SB}$
$B \lhd \{N_e, T_A\}\ S_{Key}$

طبق فرض، $B|\equiv B\leftrightarrow S$ است؛ پس B می‌تواند پیامی را که به‌واسطه A از S دریافت کرده، با کلید مشترکشان رمزگشایی کند:

$B|\equiv S|\equiv (N_c, R_{Ui}, R_{Si}, T_S)$
پس $B|\equiv R_{Si}, B|\equiv R_{Ui}$

با دانستن این مقادیر، B مقدار S_{Key} را محاسبه می‌کند. بنابراین:

$B \lhd \{N_e, T_A\}\ S_{Key}$
$B|\equiv (N_e, T_A)$
$B|\equiv T_A$

حال، B یک واحد به مقدار T_A اضافه می‌کند و آن را رمزگذاری کرده و برای A ارسال می‌کند (پیام ۴). A یک پیام از B دریافت می‌کند که با کلید S_{Key} می‌تواند آن را بخواند و به محتوای پیام دست پیدا کند:

$$A \lhd \{R_{Ui}, T_{A+1}\}\ S_{Key}$$

از اثبات ۱، با استفاده از نتیجه حاصل‌شده در رابطه (۲) داریم: $A|\equiv S_{Key}$. پس هدف ۲ نیز اثبات می‌گردد:

$A|\equiv (R_{Ui}, T_{A+1})$
$A|\equiv T_{A+1}$

با جاگذاری U به‌جای A طبق فرض ابتدایی، خواهیم داشت: $U|\equiv T_{A+1}$. نتیجه ارزیابی با استفاده از منطق بن، در اثبات ۱ و ۲، نشان می‌دهد که روش پیشنهادی پژوهش در مورد احراز هویت دوطرفه کاربر و مرجع ثبت و همچنین کاربر و گره دروازه، به‌صورت صحیح کار می‌کند.

۴-۲. ارزیابی با استفاده از ابزار آویسپا

روش پیشنهادی این تحقیق در ابزار آویسپا شبیه‌سازی‌شده و موردبررسی و ارزیابی قرارگرفته است. این ابزار معمولاً در اثبات کارایی روش‌های مربوط به امنیت در خانه هوشمند استفاده می‌شود. زبان برنامه‌نویسی این ابزار، زبان HLPSL[1] است که یک زبان سطح بالا بوده و برای اجراشدن، ابتدا به زبان HLPSL2IF ترجمه‌شده و سپس به‌عنوان ورودی در چهار مدل برنامه سرویس‌دهنده مورد استفاده قرار می‌گیرد. این مدل‌ها عبارت‌اند از OFMC[2]، CLAtSe[3]، SATMC[4]، TA4SP[5] [۱۲].

ابزار آویسپا، کاربرد زیادی در تجزیه‌وتحلیل پروتکل‌های امنیتی دارد. برای استفاده از این ابزار، مدل‌های پروتکلی باید به زبان HLPSL نوشته شوند. مرحله ثبت کاربر، و ورود/ احراز هویت در HLPSL پیاده‌سازی شده‌اند. در این پیاده‌سازی، سه نقش اصلی در نظر گرفته‌شده‌اند: کاربر که با حرف A (به‌طور مثال، حرف ابتدای Alice) مشخص‌شده است. مرجع ثبت که با حرف S (حرف ابتدای Server) مشخص‌شده است، و گره دروازه که با حرف B (حرف ابتدای Bob) مشخص‌شده است. روش پیشنهادی با استفاده از بک-اِند[6]های OFMG و CL-AtSe در آویسپا پیاده‌سازی شده است.

پس از پیاده‌سازی توسط کدهای زبان HLPSL و اجرای برنامه توسط نرم‌افزار آویسپا، نتایج به‌دست‌آمده که به ترتیب در شکل‌های (۵) و (۶) مشخص است، حاکی از قابل‌اطمینان بودن روش پیشنهادی است.

```
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL
PROTOCOL
 /home/span/span/testsuite/results/testfinal.if
GOAL
 As Specified
BACKEND
 CL-AtSe
STATISTICS
 Analysed  : 357012 states
 Reachable  : 28904 states
 Translation: 0.10 seconds
 Computation: 9.24 seconds
```

شکل (۵). شبیه‌سازی روش پیشنهادی با CL-AtSe

```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/testfinal.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 1.41s
 visitedNodes: 348 nodes
 depth: 16 plies
```

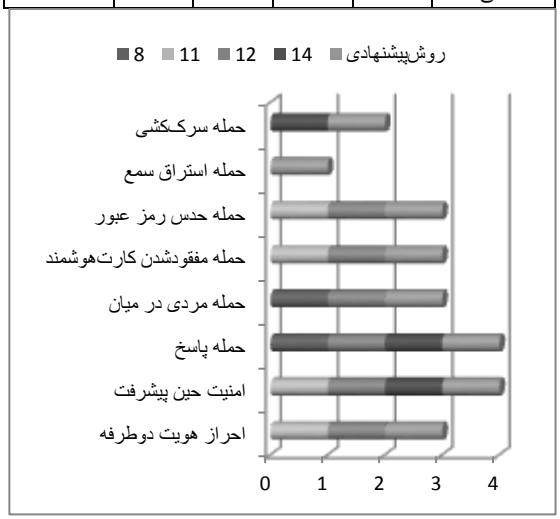
شکل ۶. شبیه‌سازی روش پیشنهادی با OFMC

[1] High Level Protocol Specification Language (زبان مشخصات پروتکل سطح بالا)
[2] On-the-fly-model-checker
[3] CL-based Attack Searcher
[4] SAT-based Model-Checker
[5] Tree Automated based on Automatic Approximations for the Analysis of Security Protocol
[6] Backend

جهت ارزیابی میزان کارایی عملکرد روش پیشنهادی در مقایسه با روش‌های موجود، نتایج آزمون‌های انجام‌گرفته بر روی روش پیشنهادی و روش‌های موجود، در جدول (۲) نشان داده شده است.

جدول ۲. ارزیابی روش پیشنهادی بر اساس عامل‌های امنیتی

عامل مقایسه	[۸]	[۱۱]	[۱۲]	[۱۴]	روش پیشنهادی
احراز هویت دوطرفه[1]	×	✓	✓	×	✓
رازداری پیش-رو[2]	×	✓	✓	✓	✓
حمله تکرار[3]	✓	×	✓	✓	✓
حمله مردی در میان[4]	✓	×	✓	-	✓
حمله مفقودشدن کارت‌هوشمند[5]	×	✓	✓	-	✓
حمله حدس رمز عبور[6]	×	✓	✓	×	✓
حمله استراق سمع[7]	×	×	×	×	✓
حمله سرک-کشی[8]	×	×	×	✓	✓



نمودار ۱. مقایسه روش پیشنهادی و روش‌های پیشین بر اساس عامل‌های امنیتی

با توجه به نتایج ارائه‌شده در جدول (۲) و نمودار (۱)، روش پیشنهادی از عامل‌های امنیتی بیشتری در مقایسه با روش‌های موجود، پشتیبانی می‌کند. جزئیات بیشتر عامل‌های مقایسه و چگونگی آزمون آن‌ها، در زیر ارائه شده است. جهت بررسی احراز هویت دوطرفه، در روش پیشنهادی، کاربر پیام را به سرویس‌دهنده ارسال می‌کند و سرویس‌دهنده، هویت او را تائید می‌کند و برای کاربر، یک پیام ارسال می‌کند. کاربر قابل‌اطمینان بودن پیام دریافت شده از طرف سرویس‌دهنده را با بررسی T، تائید می‌کند. درنتیجه، یک احراز هویت دوسویه بین کاربر و مرجع ثبت و بالعکس برقرار شده است.

ازنظر رازداری پیش‌رو، اگر کارت هوشمند دزدیده شود و به دست مهاجم بیفتد، و اگر فرض شود که مهاجم، مقدار x را نیز داشته باشد، به‌دلیل نداشتن رمز عبور کاربر نمی‌تواند پیام C را تولیدکند و برای سرویس‌دهنده بفرستد و بنابراین با شکست مواجه می‌شود. ازنظر حمله تکرار، رمز عبوری که توسط کاربر وارد می‌شود و به مرجع ثبت ارسال می‌شود، توسط تابع چکیده‌ساز یک‌طرفه F() درهم می‌شود. بنابراین، اگر مهاجم بتواند به U_{ID} دست پیدا کند، هرگز نمی‌تواند رمز عبور مربوط به آن را بیابد و با شکست مواجه می‌شود.

جهت بررسی حمله مردی در میان، فرض شود که مهاجم، پیام ورود/احراز هویت را بدون این‌که طرفین متوجه شوند، دریافت کند (مثلاً خودش را به‌جای سرویس‌دهنده جا بزند و پیام (A_{ID}, C) را از کاربر بگیرد و آن را تبدیل به (A_{ID}, C) کند و برای سرویس‌دهنده ارسال کند). زمانی که سرویس‌دهنده این پیام را دریافت می‌کند، از طریق رمزگشایی C، مقدار ID کاربر را به دست می‌آورد و با A_{ID} مقایسه می‌کند و متوجه تقلبی بودن این پیام می‌شود و درنتیجه، درخواست کاربر رد می‌شود.

وقتی یک کارت هوشمند گم و یا دزدیده می‌شود، اگر فرض شود که کاربر غیرمجاز می‌تواند با حمله حدس مکرر، رمز عبور کارت هوشمند را حدس بزند، یا بخواهد به‌جای کاربر سعی در ورود به سامانه داشته باشد، زمانی که کارت را وارد پایانه کند، اولین چالشی که با آن مواجه می‌شود، باید ابتدا یک درخواست معتبر به شکل (A_{ID}, C) را تولید کند. چون مهاجم به‌دلیل نداشتن v_i قادر به تولید کردن C نیست، بنابراین نمی‌تواند این درخواست معتبر را بسازد و روش پیشنهادی در مقابل حمله مفقود شدن کارت هوشمند، نیز مقاوم است.

در روش پیشنهادی، اگر مهاجم به درخواست ورود/ احراز هویت (A_{ID}, C) دسترسی پیدا کند، نمی‌تواند رمز عبور را حدس بزند چراکه کلید سری X را ندارد. لذا این روش در مقابل حمله

[1] Mutual authentication
[2] Forward secracy
[3] Replay attack
[4] Man-in-the middle attack
[5] Smart cart loss attack
[6] Password guessing attack
[7] Eavesdropping
[8] Shoulder surfing

حدس رمز عبور، نیز مقاوم است. همچنین اگر کاربری برای اولین بار بخواهد وارد سامانه شود یا احراز هویت شود، ممکن است برنامه‌های استراق سمع بتوانند به شناسه و رمز او دست یابند. روش پیشنهادی در برابر این حمله نیز مقاوم است چراکه تمام پیام‌های مهم مثل پیام پاسخ به درخواست ورود/ احراز هویت و بلیط احراز هویت، به ترتیب با کلیدهای R_{Ui} و K_{SB} که یک کلید متقارن است، رمزگذاری می‌شوند.

ازنظر حمله سرک‌کشی نیز، اگر فرض شود که کاربری توسط سرک‌کشی، اطلاعات یک کاربر مجاز را به دست آورده باشد، به‌دلیل این‌که مقدار R_{Ui} را نمی‌داند، نمی‌تواند پیام پاسخ به درخواست ورودش را که از سمت سرویس‌دهنده برای او ارسال می‌شود، باز کند و درنتیجه، درخواست ورود/ احراز هویت او رد می‌شود.

۵. نتیجه‌گیری

اعتماد نا به‌جا به افراد و عدم احراز هویت صحیح در خصوص فردی که قصد استفاده از خدمات خانه هوشمند را دارد، موجب هدر رفتن سرمایه‌های مالی و شاید اعتبار و آبروی اشخاص می‌شود. بنابراین، به کار بستن راه‌کاری مؤثر جهت اداره نمودن احراز هویت افراد به‌گونه‌ای که بتواند در برابر حملات مخرب بیشتری مقاومت کند و مانع ورود مهاجمین به سامانه خانه هوشمند شود، از اهمیت به‌سزایی برخوردار است.

در این مقاله، روشی مبتنی بر تلفیق رمز یکبار مصرف و کارت هوشمند و الگوریتم منحنی بیضوی جهت احراز هویت افرادی که قصد ورود به سامانه خانه هوشمند را دارند، ارائه گردید. روش پیشنهادی، احراز هویت متقابل بین کاربر و گره دروازه و همچنین اشیا خانه هوشمند و گره دروازه، را انجام می‌دهد. ارزیابی‌های انجام‌شده حاکی از آن است که روش پیشنهادی در مقایسه با روش‌های موجود، قادر است با تعداد حمله متداول بیشتری به خانه هوشمند، مقابله نماید.

۶. مرجع‌ها

[1] Bugeja, J.; Jacobsson, A.; Davidsson, P. "On Privacy and Security Challenges in Smart Connected Homes"; European Intelligence and Security Informatics Conference (EISIC), 2016, 172-175.

[2] Robles, R. J.; Kim, T.h.; Cook, D.; Das, S. "A Review on Security in Smart Home Development"; IJAST. 2010, 15, 14-29

[3] Saleh, E. ; Abou, A. "An IDS for Detection of Active Attacks Against Rouring in Mobile Ad-Hoc Networks"; Journal of advanced defence science and technology. 2010, 1, 15-22.

[4] Ashibani, Y.; Kauling, D.; Mahmoud, Q. H. "A Context-Aware Authentication Framework for Smart Homes"; IEEE 30th Canadian Conf. Electrical and Computer Eng. (CCECE). 2017, 1-5.

[5] Frank, M.; Biedert, R.; Ma, E.; Martinovic, I.; Song, D. "Touchalytics: On the Applicability of Touchscreen Input As A Behavioral Biometric for Continuous Authentication"; IEEE Trans. Inf. Forensics Security. 2012, 8, 136-148

[6] Song, T.; Li, R.; Mei, B.; Yu, J.; Xing, X.; Cheng, X. "A Privacy Preserving Communication Protocol for Iot Applications in Smart Homes"; IEEE Internet Things J 2017, 4, 1844-1852

[7] Vandana, C.; Imam, T.; Dubey, S. "Security Issues in Home Automation"; IJSRCSEIT. 2017

[8] Jeong, J.; Chung, M. Y.; Choo, H. "Integrated OTP-based User Authentication Scheme Using Smart Cards in Home Networks"; Proc. 41st Annual Hawaii Int. Conf. System Sciences (HICSS). 2008, 294-294.

[9] Vaidya, B.; Park, J. H.; Yeo, S.S.; Rodrigues, J. J. "Robust one-time Password Authentication Scheme Using Smart Card for Home Network Environment"; Comput Commu.n 2011, 34, 326-336

[10] Santoso, F. K. ; Vun, N. C. "Securing IoT for smart home system"; Int. Symposium on Consumer Electronics (ISCE). 2015, 1-2.

[11] Chang, C.-C. ; Le, H.D. "A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad Hoc Wireless Sensor Networks"; IEEE T Wirel Commun. 2015, 15, 357-366.

[12] Das, A. K.; Kumari, S.; Odelu, V.; Li, X.; Wu, F.; Huang, X. "Provably secure User Authentication and Key Agreement Scheme for Wireless Sensor Networks"; Secur Commun Netw. 2016, 9, 3670-3687.

[13] Wazid, M.; Das, A. K.; Odelu, V.; Kumar, N.; Susilo, W. "Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment"; IEEE Trans. Depend. Sec. Comput. 2017.

[14] Kumar, P.; Gurtov, A.; Iinatti, J.; Ylianttila, M.; Sain, M. "Lightweight and secure Session-Key Establishment Scheme in Smart Home Environments"; IEEE Sensors J. 2015, 16, 254-264.

[15] Li, Y. "Design of a Key Establishment Protocol for Smart Home Energy Management System"; Fifth Int. Conf. Comput. Intell. Commun. Syst. Netw. 2013, 88-93.

[16] Sierra, JM.; Hernández ,JC.; Alcaide, A.; Torres, J. "Validating the Use of BAN LOGIC"; Int. Conf. Comput. Sci. Appl. 2004,5, 851-858.

[17] Masoumi, M.; Mahdizadeh, H. "The FPGA Implementation of an Efficient Elliplic Curve Cryptographic Process over GF(2163)"; Advanced Defence Sci.& Tech., 2012, 3, 199-211.

[18] Naoui, S.; Elhdhili, M.E.; Saidane, L.A.; "Lightweight and Secure Password Based Smart Home Authentication Protocol: LSP-SHAP"; J NETW SYST MANAG. 2019, 4, 1020-1042.

[19] Shuai, M.; Yu, N.; Wang, H.; Xiong, L.; "Anonymous Authentication Scheme for Smart Home Environment Provable Security"; COMPUT SECUR. 2019, 132-146.

[20] Gurabi, M.A.; Alfandi, O.; Bochem, A.; Hogrefe, D.; "Hardware based Two-Factor User Authentication for the Internet of Things"; IWCMC.2018, 4, 1081-1086.