Journal of Electronical & Cyber Defence
Vol. 9, No. 2, 2021, Serial No. 34

A Mutual Authentication Protocol for IoT Users in Cloud Environment

A. Shahidinejad

* Qom Islamic Azad University

(Received: 06/07/2020, Accepted: 11/012021)

ABSTRACT

Ensuring the security of the Internet of Things (IoT) services and the related applications is crucial in building users' trust in utilizing the Internet of Things platform. Data generated from various smart devices on the Internet of Things is one of the biggest concerns. Cloud computing has emerged as a critical technology that can process such a large database repository of various devices available on the Internet of Things. Authentication and privacy of IoT-enabled devices play a critical role in integrating the IoT and cloud computing technologies. The complexity and robustness of authentication protocols are still the major challenges. This article provides a mutual authentication protocol for IoT-enabled devices. AVISPA is used to evaluate the proposed protocol's performance formally, and the MatLab tool is used to evaluate the time and communication costs. The results show the superiority of the proposed protocol compared to other approaches in terms of speed and robustness.

Keywords: Internet of Things, Cloud Computing, Authentication Protocol

* Corresponding Author Email: a.shahidinejad@qom-iau.ac.ir

نشریه علمی "پدافند الکترونیکی و سایبری"
سال نهم، شماره ۲، تابستان ۱۴۰۰، ص ۲۸-۱۷

علمی – پژوهشی

پروتکل احراز هویت متقابل برای کاربران اینترنت اشیا در محیط ابری

علی شهیدی‌نژاد*

استادیار، گروه مهندسی کامپیوتر، واحد قم، دانشگاه آزاد اسلامی، قم، ایران

(دریافت: ۱۳۹۹/۰۴/۱۶، پذیرش: ۱۳۹۹/۱۰/۲۲)

چکیده

تضمین امنیت خدمات و کاربردهای اینترنت اشیا، فاکتور بسیار مهمی در ایجاد اعتماد در کاربران و به‌کارگیری بستر اینترنت اشیا می‌باشد. داده‌های تولیدشده از دستگاه‌های مختلف هوشمند در اینترنت اشیا یکی از بزرگ‌ترین نگرانی‌ها به حساب می‌آیند. برای پردازش یک چنین مخزن پایگاه داده‌ای بزرگ که از انواع دستگاه‌های موجود در اینترنت اشیا تولید شده، رایانش ابری به‌عنوان یک فناوری کلیدی پدید آمده است، احراز هویت و حریم خصوصی دستگاه‌هایی با قابلیت IoT، نقش اساسی در موفقیت ادغام اینترنت اشیا و فناوری‌های رایانش ابری ایفا می‌کند. پیچیدگی و استحکام پروتکل‌های احراز هویت هنوز از چالش‌های اصلی است. در این مقاله، یک پروتکل احراز هویت متقابل برای کاربران خدمات اینترنت اشیا ارائه می‌شود. برای ارزیابی رسمی عملکرد پروتکل، از ابزار AVISPA استفاده می‌شود و برای تحلیل هزینه زمانی و هزینه ارتباطی پروتکل از MatLab استفاده می‌شود. نتایج حاکی از برتری پروتکل پیشنهادی نسبت به سایر رویکردها از نظر سرعت و استحکام است.

کلیدواژه‌ها: اینترنت اشیا، رایانش ابری، پروتکل احراز هویت

۱- مقدمه

اینترنت اشیا مفهومی رایانشی است برای توصیف آینده‌ای که در آن اشیای فیزیکی یکی پس از دیگری به اینترنت متصل خواهند شد و با اشیای دیگر در ارتباط قرار می‌گیرند، شامل فناوری‌های حسگر، فناوری‌های بی‌سیم، کدهای واکنش سریع نیز می‌شوند. فناوری‌های اینترنت اشیا[1] کاربردهای متنوعی در حوزه‌های سلامت، صنعت، ساختمان‌های هوشمند و شهرهای هوشمند داشته و هریک از این کاربردها، نیازهای امنیتی خاص خود را دارند. دو ویژگی اصلی مشخصه هویتی و ارتباط اینترنتی می‌تواند اشیا مختلف را به‌عنوان بخشی از اینترنت اشیا قرار دهد. هر کدام از این اشیا هوشمند، یک آدرس پروتکل اینترنتی (IP) مختص به خود را خواهند داشت تا ابزاری که به ارسال یا دریافت اطلاعات می‌پردازد، قابل تشخیص شود [۱]. با رشد اینترنت اشیا هر روزه تعداد بیشتری دستگاه به محیط اینترنت متصل می‌گردند نه تنها تعداد اشیا زیاد است، بلکه داده‌هایی که به‌وسیله هر شی نیز تولید می‌شود بسیار حجیم است. اینترنت اشیا، به‌شدت در برابر انواع حملات آسیب‌پذیر است این آسیب‌پذیری به‌دلیل این واقعیت است که اکثر ارتباطات در آن بی‌سیم هستند که ریسک استراق سمع را افزایش می‌دهد. علاوه‌براین، اکثر دستگاه‌های موجود در شبکه اینترنت اشیا، ازنظر قابلیت‌های منابع محاسباتی، ذخیره‌سازی و انرژی محدود هستند این محدودیت‌ها ناشی از کمبود پهنای باند به جهت وجود نرخ داده بالاتر و مشکلات مرتبط با سربارهای ارتباطی می‌باشد. بنابراین، اینترنت اشیا انواع پروتکل‌های امنیتی پیچیده را نمی‌تواند پشتیبانی کند. مسائل امنیتی، مهم‌ترین مانع برای توسعه این محیط‌ها محسوب می‌شوند. یکی از مسائل امنیتی، احراز هویت موجودیت‌های مختلف در اینترنت اشیا می‌باشد. احراز هویت، مهم‌ترین نقش را در ادغام موفقیت‌آمیز دستگاه‌های شبکه اینترنت اشیا و خدمات محاسبات ابری بازی می‌کند. موضوع امنیت و حریم خصوصی، به‌عنوان یک مشکل اساسی بر سر راه اینترنت اشیا به شمار می‌رود. از آنجایی که احراز هویت معمولاً نیازمند وجود سرورها و زیرساخت‌های مناسب برای تبادل پیام میان اجزای مختلف است، تأمین آن در اینترنت اشیا کار دشواری است. نیازمندی‌های امنیتی بر اساس لایه شبکه و نوع کاربرد متفاوت هستند و استخراج دقیق این نیازمندی‌ها بنا بر شرایط، نیازمند بررسی بسیار کلی و جامع است. از جمله شرایطی که نیازمندی‌های

* رایانامه نویسنده مسئول: a.shahidinejad@qom-iau.ac.ir

[1] Internet of Things (IoT)

ناشر: دانشگاه جامع امام حسین (ع)

امنیتی در آن‌ها می‌تواند متفاوت باشد، مانند استفاده از RFID، شبکه‌های حسگر، سامانه‌های بی‌سیم، شبکه‌های پوششی، سامانه‌های بیدرنگ، سامانه‌های قابل اطمینان، بسترهای فیزیکی و منطقی ارسال اطلاعات، درگاه‌های ارتباطی، ساختار شبکه (مرکزی و غیرمرکزی)، تعداد عناصر و ساختار آنها، میزان اهمیت یک سیستم یا دستگاه، مسیریابی، ترافیک‌های عبوری و ازدحام، و پروتکل‌های امنیتی مورد استفاده است. تأمین امنیت شبکه‌های ناهمگن در اینترنت اشیا کار دشواری است. روش‌های متداول تأمین امنیت که اغلب متمرکز نیز هستند، ممکن است پاسخگو نباشد و باید روش‌های جدید سبک‌وزنی توسعه داده شوند. به‌دلیل محدودیت منابع انرژی، ذخیره‌سازی و محاسباتی در شبکه‌های IoT نمی‌توان از پروتکل‌های امنیتی قدرتمند با بار محاسباتی سنگین و پیچیدگی محاسباتی زیاد برای این شبکه‌ها استفاده کرد، به‌همین دلیل این پژوهش بر آنست که پروتکل امنیتی سبک‌وزنی (با بار محاسباتی کم) و در عین حال مستحکم در برابر حملات را ارئه دهد.

سهم علمی این پژوهش به شرح زیر می‌باشد:

- ارائه پروتکل احراز هویت متقابل در چارچوب محیط ابر توزیع‌شده
- اعتبارسنجی رسمی امنیت پروتکل با محیط شبیه‌سازی AVISPA

سازمان‌دهی ادامه مقاله بدین صورت می‌باشد، در بخش دوم مقاله، کارهای مرتبط در زمینه طرح‌های احراز هویت برای دستگاه‌های دارای قابلیت اینترنت اشیا ارائه می‌شود. در بخش سوم به شرح پروتکل پیشنهادی پرداخته می‌شود. در بخش چهارم، نتایج عملکرد پروتکل پیشنهادی در قالب نتایج شبیه‌سازی مورد ارزیابی قرار گرفته و در نهایت، در بخش پنجم نتیجه‌گیری و پیشنهادها مطرح می‌گردد.

۲- ادبیات تحقیق

تحقیقات متنوعی در مورد پروتکل‌های احراز هویت سبک‌وزن در حوزه شبکه‌های اینترنت اشیا و امنیت در اینترنت اشیا توسط محققان انجام گرفته است که در ذیل بخشی از آن‌ها معرفی می‌شوند:

آلامر و همکارانش [۲] یک پروتکل احراز هویت متقابل RFID[1] بر اساس رمزنگاری منحنی بیضوی (ECC[2]) برای اینترنت اشیا به‌منظور حذف تهدیدات امنیتی ناشی از کانال ناامن بین برچسب و قرائت‌گر ارائه دادند. علاوه‌براین، از پروتکل مبادله کلید ECDH[3] برای تولید کلید موقتی اشتراکی برای رمزنگاری پیام‌های جدید انتقال داده شده استفاده می‌کند. تحلیل امنیتی پروتکل پیشنهادی نشان می‌دهد که پروتکل پیشنهادی ویژگی‌های امنیتی مانند احراز هویت متقابل، گمنامی، محرمانگی، امنیت پیشرو[4]، حریم خصوصی مکان[5] را تضمین می‌کند و همچنین در مقابل حملات جعل هویت، تکرار و مرد میانی مقاوم می‌باشد.

کالرا و همکارانش [۳] پروتکل احراز هویت متقابل برای دستگاه‌های تعبیه‌شده و سرورهای ابری بر اساس رمزنگاری منحنی بیضوی پیشنهاد کردند. پروتکل پیشنهادی، احراز هویت بین دستگاه و خدمات‌دهنده ابری را با استفاده از کوکی‌های HTTP تضمین می‌کند. این پروتکل نیازمندی‌های امنیتی احراز هویت متقابل، محرمانگی، گمنامی و امنیت پیشرو را تضمین می‌کند و در برابر حملات امنیتی مانند حمله تکرار، حمله مرد میانی، حمله سرقت کوکی، حمله استراق سمع، حمله جستجوی فراگیر، حمله دیکشنری برون‌خط و حمله نشت تصدیق‌کننده مقاوم می‌باشد. الگوریتم‌های رمزنگاری مبتنی بر منحنی بیضوی، راه‌حل‌های امنیتی بهتری در مقایسه با دیگر الگوریتم‌های رمزنگاری کلید عمومی (PKC[6]) به‌دلیل اندازه کلید کوچک‌تر و محاسبات کاراتر ارائه می‌کنند و برای محیط‌هایی با دستگاه‌های منبع محدود ازنظر حافظه و قدرت پردازشی بسیار مناسب هستند.

در مقاله [۴]، نویسندگان پروتکل ارائه شده توسط وو و همکاران [۵] را بررسی کردند و نشان دادند که محرمانگی پیشرو را ارضا نمی‌کند و از تهدیدات ربودن کارت هوشمند و حمله داخلی مجاز شده رنج می‌برد. برای مقابله با محدودیت‌های امنیتی ذکر شده، آن‌ها یک پروتکل احراز هویت پیشرفته مبتنی بر تغییر کلید را برای شبکه سرور ابری توزیع‌شده در شبکه 5G اینترنت اشیا پیشنهاد داده‌اند. آن‌ها تجزیه و تحلیل امنیتی رسمی پروتکل پیشنهادی خود را با استفاده از ابزار ProVerif و مدل منطق BAN انجام دادند و نشان دادند که این سامانه ایمن است. علاوه‌براین، مقایسه عملکرد نشان می‌دهد که پروتکل پیشنهادی آن‌ها از لحاظ هزینه‌های محاسباتی تابع چکیده‌ساز نسبت به آخرین طرح‌های احراز هویت بهتر عمل می کند.

یو و همکاران [۶]، طرح ارائه شده توسط هی و همکاران [۷] را تجزیه و تحلیل کردند و ثابت کردند که در برابر حملات DoS و حمله داخلی مجاز شده آسیب‌پذیر است. بنابراین، آن‌ها توافق‌نامه کلید پیشرفته و طرح احراز هویت را برای شبکه ابری

[1] Radio-Frequency Identification
[2] Elliptic Curve Cryptography

[3] Elliptic Curve Diffie–Hellman
[4] Forward Security
[5] Location Privacy
[6] Public Key Cryptography

مبتنی بر IoT طراحی کردند. طرح پیشنهادی آن‌ها از تاییدکننده فازی برای اصلاح مراحل ثبت و احراز هویت طرح پیشنهادی برای محافظت در برابر حملات امنیتی مشهور استفاده کرده است. آن‌ها جنبه‌های امنیتی خودکار طرح پیشنهادی خود را با استفاده از ابزار ProVerif مورد تجزیه و تحلیل قرار داده و اثبات‌ها را از طریق مدل منطق BAN ارائه دادند تا مقاومت پروتکل پیشنهادی خود را در برابر حملات مختلف اثبات کنند. سرانجام، نتایج تجزیه و تحلیل عملکرد و امنیت نشان داد که طرح احراز هویت آن‌ها بسیار مطمئن‌تر از طرح اولیه است اما از نظر هزینه محاسباتی اندکی بالاتر است.

کمیسا و همکارانش [۸] پروتکلی پیشنهاد دادند که با توجه به گسترش اینترنت اشیا، درهای زیادی را به سمت کاربردهای مختلف خواهد گشود. شبکه‌های حسگر بی‌سیم (WSN) به‌عنوان یکی از واقعی‌ترین و مؤثرترین کاربردهای شبکه اینترنت اشیا می‌باشند. این تحقیق بر روی تعامل بین گره حسگر با کاربر راه دور متمرکز شده و یک پروتکل سبک‌وزن برای این محیط‌های منبع محدود ارائه می‌دهد. پروتکل پیشنهادی این امکان را فراهم می‌کند که گره حسگر و کاربر راه دور به یک روش امن یکدیگر را احراز هویت کنند. پروتکل پیشنهادی از رشته اعداد تصادفی، عملیات XOR و HMAC[1] برای بررسی یکپارچگی پیام‌های مبادله شده استفاده می‌کند. تحلیل امنیتی نشان می‌دهد پروتکل پیشنهادی در مقابل انواع حملات مقاوم بوده و بسیاری از نیازمندی‌های امنیتی را برآورده می‌کند.

تورکانوویچ و همکاران [۹] یک تابع چکیده‌ساز مبتنی بر احراز هویت کاربر و پروتکل توافق‌نامه کلید برای حسگرهای بی‌سیم متصل به‌منظور دست‌یابی به انرژی کمتر، احراز هویت متقابل، ناشناس بودن کاربر و سایر ویژگی‌های امنیتی پیشنهاد کردند. متأسفانه، امین و بیسوا [۱۰] به برخی از نقاط ضعف امنیتی در [۹] از جمله حمله سرقت کارت هوشمند، حملات حدس زدن رمز- هویت خارج از خط، حمل جعل هویت گره حسگر، حمله جعل هویت کاربر و موارد دیگر اشاره کرد. برای برطرف کردن چنین اشکالات امنیتی، آن‌ها طرحی که می‌تواند بسیاری از نگرانی‌های امنیتی از جمله نیاز به انرژی کمتر، احراز هویت متقابل، ناشناس بودن کاربر و مرحله تغییر رمز مساعد کاربر را تحمل کند، طراحی کردند.

امین و همکاران [۱۱] یک طرح تائید هویت گسترده برای دستگاه‌های IoT در سامانه‌های ابر جغرافیایی توزیع‌شده طراحی کرده‌اند. آنها پروتکل [۱۲] را مورد مطالعه قرار داده و اعلام کردند که این پروتکل در برابر حملات افشای کلید جلسه و جعل هویت کاربر مقاومت نمی‌کند و برخی از الزامات امنیتی مانند ناشناس بودن کاربر در آن ارائه نشده است. بنابراین، آن‌ها چارچوبی را طبق سامانه ابری توزیع‌شده جغرافیایی برای ذخیره و بازیابی کلیه اطلاعات محرمانه از سرورهای ابری خصوصی پیشنهاد دادند. همچنین، آن‌ها طرح احراز هویت پیشنهادی خود را با استفاده از مدل منطق BAN و ابزار AVISPA تائید کردند و نشان دادند که در برابر حملات امنیتی از جمله جعل هویت کاربر، حدس زدن رمز عبور برون‌خط، افشای کلید جلسه، حمله داخلی مجاز شده و حملات تکرار محفوظ است.

فنگ و همکاران [۱۳] یک روش احراز هویت بر اساس تابع چکیده‌ساز برای محیط اینترنت اشیا پیشنهاد دادند و ادعا کردند که این روش از امنیت خوبی برخوردار است اما لیمباسیا و همکاران [۱۴] مشاهده کردند که برخی نقطه ضعف امنیتی دارد در نتیجه تحقق عملی آن بسیار سخت است. آن‌ها یک طرح احراز هویت سبک‌وزن طراحی کردند که در برابر چندین چالش امنیتی در زندگی واقعی مقاوم می‌باشد.

کومار و همکاران [۱۵] برای حمایت تبادل کلید بین سرورهای ابری و برچسب‌های RFID در شبکه رایانش ابری، یک طرح احراز هویت امن پیشنهاد کرده‌اند. آن‌ها از ECC برای برقراری ارتباط امن با ویژگی ناشناس بودن استفاده کردند. علاوه‌براین، آن‌ها به‌طور رسمی تجزیه و تحلیل امنیتی طرح پیشنهادی خود را با استفاده از ابزار AVISPA در مدل اوراکل تصادفی انجام داده‌اند و نشان داده‌اند که در برابر حملات مرد میانی و تکرار ایمن است. همچنین، نتایج تجزیه و تحلیل عملکرد در مورد کار پیشنهادی خود، عملکرد خوبی را از نظر سربار محاسبات و هزینه‌های ارتباطی در مقایسه با طرح‌های موجود ارائه می‌دهد.

ژو و همکاران [۱۶] پروتکل احراز هویت جدیدی را برای سامانه‌های دارای قابلیت IoT با کمک ابر ارائه دادند. آن‌ها عمل XOR و تابع چکیده‌ساز یک‌طرفه را در پروتکل پیشنهادی خود برای تقویت ویژگی‌های امنیتی استفاده و تصویب کردند. آن‌ها راه‌حل خود را از طریق تجزیه و تحلیل تائید رسمی با استفاده از ابزار Proverif ارزیابی کردند و ثابت کردند که در برابر حملات معروف شناخته شده ایمن است و ویژگی‌های امنیتی از جمله امنیت جلسه، بازرسی کاربر و احراز هویت متقابل را فراهم می‌کند. همچنین، نتایج عملکرد آن‌ها از نظر هزینه محاسبه عملیات رمزنگاری نشان می‌دهد که پروتکل پیشنهادی آن‌ها عملی است.

وزید و همکاران [۱۷] یک سازوکار احراز هویت سبک‌وزن را برای دسترسی به داده‌های دستگاه‌های IoT در محیط اینترنت

[1] Hash-based Message Authentication Code

اشیا مبتنی بر ابر ایجاد کرده‌اند. سازوکار پیشنهادی آن‌ها از عملیات XOR و توابع چکیده‌ساز یک‌طرفه با استخراج فازی برای تائید بیومتریک کاربران نهایی در مرحله ورود به سامانه، استفاده کرده است. آن‌ها جنبه‌های امنیتی سازوکار خود را از طریق تائید امنیت رسمی با استفاده از ابزار AVISPA تجزیه و تحلیل کردند و نشان دادند که در برابر حمله تکرار، جعل هویت، مرد میانی، تغییر رمز عبور و حملات DoS مقاومت می‌کند. همچنین، نتایج شبیه‌سازی آن‌ها با استفاده از شبیه‌ساز NS2 نشان داد که از نظر اعتبار عملکرد سازوکار هزینه‌های ارتباطی، هزینه محاسبه و عملکرد شبکه در مقایسه با پروتکل‌های احراز هویت موجود بهتر عمل می‌کند.

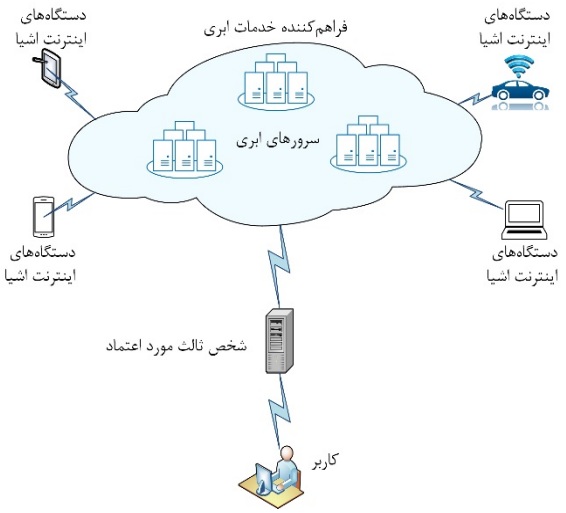
در تحقیقات گذشته، پروتکل‌های سبک‌وزن در برابر تعدادی از حملات نفوذپذیر هستند و پروتکل‌هایی که در برابر تمامی حملات قابل نفوذ نیستند نیز سربار محاسباتی و ارتباطی سنگینی دارند. به همین منظور در این مقاله هر دو عامل استحکام در برابر حملات و سربارهای محاسباتی و ارتباطی در طراحی پروتکل لحاظ شده است.

۳- روش پیشنهادی

همان‌طور که در مقدمه اشاره شد، با توجه به بالا بودن حجم اطلاعات تولیدشده در اینترنت اشیا، نگهداری و امنیت داده‌ها حائز اهمیت می‌باشد، این پژوهش با پروتکل احراز هویت سبک‌وزن و استفاده از معماری سه لایه، شامل کاربران، شخص ثالث مورد اعتماد و فراهم‌کننده خدمات ابری طراحی شده است.

۳-۱- معماری روش پیشنهادی

شکل (۱) معماری محیط ابر توزیع‌شده را نمایش می‌دهد. عناصر اصلی روش پیشنهادی عبارت‌اند از: کاربران، شخص ثالث مورد اعتماد و فراهم‌کننده خدمات ابری. روال کلی به این شکل می‌باشد که کاربران برای درخواست خدمات از فراهم‌کننده خدمات ابری نیاز به برقراری ارتباط دارند، جهت ایجاد این ارتباط بایستی در مرکز شخص ثالث مورد اعتماد ثبت‌نام آن‌ها انجام شود و پس از ذخیره اطلاعات در پایگاه داده، شناسه منحصر به فرد و کلمه عبوری به کاربر اختصاص داده می‌شود که با این اطلاعات می‌تواند به شبکه ورود کرده و احراز هویت شود. به هر خدمات‌دهنده ابری نیز شناسه منحصر به فرد اختصاص داده می‌شود. پس از احراز هویت مرکز شخص ثالث مورد اعتماد برای رمز کردن پیام‌ها و محاسبات ارتباطی با کاربرها و خدمات‌دهنده‌های ابری از عدد امنیتی و عدد تصادفی مختص هر یک و نیز عملیات رمزنگاری استفاده می‌کند تا ارتباط امن برقرار شود.



شکل (۱): معماری روش پیشنهادی.

فرض کنید تعدادی کاربر وجود دارد که نیاز به دریافت خدمات از خدمات‌دهنده‌های ابری می‌باشند. برای دریافت خدمات جهت کنترل تکراری نبودن، جعلی نبودن و کنترل دیگر مسائل امنیتی نیاز به احراز هویت می‌باشد. بنابراین کاربران در ابتدا بایستی در شخص ثالث مورد اعتماد ثبت‌نام کنند. پس از ثبت‌نام برای ورود به شبکه جهت دریافت خدمات توسط شخص ثالث مورد اعتماد احراز هویت شده و سپس می‌توانند درخواست خود را به مرکز خدمات‌دهنده ابری ارسال کنند. جهت برقراری ارتباط امن بین کاربران و خدمات‌دهنده‌های ابری نیاز به کلید سری می‌باشد که پس از دریافت کلید، ارتباط برقرار شده و پاسخ از خدمات‌دهنده ابری دریافت خواهد شد.

خدمات‌دهنده‌های ابری نیز برای انجام عملیات در داخل شبکه نیاز به ثبت‌نام در مرکز شخص ثالث مورد اعتماد دارند. چنانچه درخواستی از کاربری دریافت کنند درخواست را به مرکز شخص ثالث مورد اعتماد ارسال می‌کنند پس از تائید هویت کاربر توسط شخص ثالث مورد اعتماد، کلید برقراری ارتباط با کاربر را دریافت می‌کنند و بر پایه احراز هویت کاربران به درخواست آن‌ها پاسخ می‌دهند.

عملیات ثبت‌نام جهت صدور مجوز ورود کاربرها و خدمات‌دهنده‌های ابری به شبکه با ذخیره اطلاعات در پایگاه داده صورت می‌پذیرد و بر اساس اطلاعات ثبت‌شده احراز هویت متقابل انجام می‌شود. برای برقراری ارتباط امن بین کاربران و خدمات‌دهنده‌های ابری نیاز به تولید کلید ارتباطی می‌باشد که با دریافت درخواست ارتباط کاربر، این کلید تولید و ارسال می‌شود.

۳-۲- پروتکل احراز هویت پیشنهادی

روش پیشنهادی شامل مراحل ثبت‌نام، ورود و احراز هویت می‌باشد. جدول (۱) متغیرهای مورد استفاده در ساختار روش پیشنهادی را معرفی می‌کند.

جدول (۱): متغیرها و تعاریف آن‌ها.

نام	تعریف
U_i	کاربر i ام
TTP	شخص ثالث مورد اعتماد
SP_j	خدمات‌دهنده ابری j ام
UID_i	شناسه کاربر i ام
P_i	کلمه عبور کاربر i ام
$SPID_j$	شناسه خدمات‌دهنده j ام
x, y	اعداد سری مرکز ثالث مورد اعتماد
c_i	عدد تصادفی انتخاب شده برای کاربر i ام
d	عدد تصادفی انتخاب شده برای SP_j
h()	تابع Hash رمزنگاری یک‌طرفه
TS	برچسب زمانی
$\oplus$	عملگر XOR
$\|\|$	عملگر الحاق

U_i متغیر مربوط به کاربر است که به‌طور مشخص هر کاربر برای هر نوع درخواست خدمات از مدیریت کاربران استفاده می‌کند. شخص ثالث مورد اعتماد به‌عنوان مدیریت اعتماد TTP نام دارد. متغیر SP معرف فراهم کننده خدمات است. کاربران دارای شناسه‌ای یکتا با نام UID و کلمه عبور P است. به‌همین ترتیب شناسه خدمات‌دهنده ابر SPID در نظر گرفته شده است. مرکز شخص ثالث مورد اعتماد برای رمز کردن پیام‌ها و محاسبات ارتباطی با کاربران از اعداد سری x و برای رمز کردن پیام‌ها و محاسبات ارتباطی با خدمات‌دهنده از عدد امنیتی y استفاده می‌کند. اعداد تصادفی c_1, c_2 برای مشخص کردن تعداد کاربران و عدد تصادفی d برای مشخص کردن تعداد خدمات‌دهندگان جهت رمزنگاری استفاده می‌گردد. تابع h() معرف یک تابع رمزنگاری چکیده‌ساز یک‌طرفه و غیرقابل بازگشت است. متغیر TS برای معرفی زمان (برچسب زمانی) در نظر گرفته شده است، بدین معنی که لحظه زمانی را برای هر عامل در نظر می‌گیرد. نماد $\oplus$ برای عملگر XOR و نماد $\|\|$ برای عملگر الحاق استفاده می‌شود. در ادامه مراحل پروتکل پیشنهادی شامل ثبت‌نام، ورود و احراز هویت با جزئیات بیشتر مورد بررسی قرار می‌گیرد.

۳-۲-۱- ثبت‌نام

در مرحله ثبت‌نام، هر کاربر و یا هر فراهم‌کننده خدمات ابتدا می‌بایست در مرکز شخص ثالث مورد اعتماد (TTP) ثبت‌نام نمایند. بدین ترتیب فراهم‌کننده خدمات ابری j ام (SP_j) با ورود به شبکه، ابتدا شناسه‌ای با نام $SPID_j$ برای خود انتخاب می‌کند. سپس شناسه و مقدار تصادفی انتخابی خود با نام d_j را تحت پیامی جهت ثبت‌نام حاوی (SID_j, d_j) برای TTP ارسال می‌کند. مرکز اعتماد پس از دریافت این پیام، با استفاده از عدد y که جهت رمزنگاری محاسبات برای فراهم‌کنندگان خدمات استفاده می‌شود، دو مقدار $PSPID_j$ و BPS_j را با استفاده از رابطه (۱) محاسبه می‌کند.

$$\begin{aligned} PSPID_j &= h(SPID_j \| d_j), \\ BPS_j &= h(PSID_j \| y \| PSPID_j) \end{aligned} \quad (۱)$$

در ادامه مرکز اعتماد مقدار BPS_j را برای خدمات‌دهنده ابری j ام ارسال می‌کند. خدمات‌دهنده j ام پس از دریافت پیام دو مقدار BPS_j و d_j را در حافظه خود ذخیره می‌کند.

اولین بار که کاربر i ام در TTP ثبت‌نام می‌کند، برای دریافت خدمات شبکه، شناسه‌ای با نام UID_i و کلمه عبوری با عنوان P_i برای خود انتخاب می‌کند. سپس با استفاده از تابع رمزنگاری h()، مقدار تصادفی انتخابی خود با نام c_i چکیده‌ساز کرده و با کلمه عبور خود P_i، XOR می‌کند و مقدار A_i را از رابطه (۲) محاسبه می‌کند.

$$A_i = P_i \oplus h(c_i) \quad (۲)$$

سپس پیامی جهت ثبت‌نام حاوی (UID_i, A_i, c_i) برای TTP ارسال می‌کند. TTP پس از دریافت این پیام، با استفاده از عدد x که جهت رمزنگاری محاسبات برای کاربر استفاده می‌شود، دو مقدار $(M_i, PUID_i, N_i, O_i)$ را با استفاده از رابطه (۳) محاسبه می‌کند و به کاربر i برمی‌گرداند.

$$\begin{aligned} PUID_i &= h(UID_i \| c_i), \\ M_i &= h(PUID_i \| A_i), \\ T_i &= h(PUID_i \| x), \\ N_i &= T_i \oplus A_i, \\ O_i &= h(PUID_i \| UID_i \| x) \end{aligned} \quad (۳)$$

TTP سپس اطلاعات مربوط به کاربر i را در بانک اطلاعاتی خود ذخیره می‌شود تا در هر نوع ارتباط با سطوح بالاتر از آن استفاده کند.

۳-۲-۲- ورود

کاربر برای دریافت خدمات باید توسط TTP تائید شود. بدین ترتیب کاربر با ورود به شبکه ارتباطی UID و کلمه عبور خود را تحت عنوان متغیر P_i^* وارد می‌کند. ابتدا در مرحله ورود مقدار A_i^* طبق رابطه (۴) محاسبه می‌گردد.

$$A_i^* = h(P_i^* + b_i) \quad (۴)$$

سپس با استفاده از A_i^* مقدار M_i^* طبق رابطه (۵) محاسبه می‌شود.

$$M_i^* = h(UID_i + A_i^*) \quad (۵)$$

در صورتی که مقدار حاصل‌شده M_i^* با مقدار M_i موجود در TTP برابر بود، کاربر رمز را صحیح وارد کرده و به او اجازه ورود به سامانه داده می‌شود. در غیر این صورت ارتباط کاربر با شبکه قطع می‌شود.

۳-۲-۳- احراز هویت

ارسال هر نوع درخواست از کاربر به خدمات‌دهنده ابری نیاز به احراز هویت کاربر دارد. بدین ترتیب که ابتدا خدمات‌دهنده برای احراز هویت و اطمینان از امن بودن ارتباط با کاربر، پیامی برای TTP ارسال می‌کند تا هویت کاربر تائید و سطح دسترسی آن مشخص گردد. در این بخش نحوه احراز هویت کاربر و ارائه کلید مشترک توسط TTP برای ارتباط بین کاربر و فراهم‌کننده خدمات ابری تشریح می‌گردد.

هنگامی‌که SP_j پیام ورود را دریافت می‌کند، ابتدا مهر زمانی را بررسی می‌کند که باطل نشده باشد. اگر مهر زمانی باطل نشده باشد مقدار N_j را به‌صورت تصادفی انتخاب می‌کند و V_i و Z_i را از رابطه (۶) محاسبه می‌کند.

$$V_i = BPS_j \oplus N_j \quad (۶)$$

$$Z_i = h(N_j \| BPS_j \| TS_j \| PUID_i \| O_i)$$

سپس SP_j مقادیر $(V_i, Z_i, M_i, PSPID_j, PUID_i, N_i, TS_j, O_i)$ را برای TTP ارسال می‌کند. در ابتدا TTP مهر زمانی را چک می‌کند که منقضی نشده باشد. در صورت صحت مهر زمانی، TTP مقادیر رابطه (۷) را محاسبه می‌کند.

$$D_i = h(PUID_i \| x),$$
$$UID_i = D_i \oplus N_i, \quad (۷)$$
$$PN_i = h(PUID_i \| UID_i \| x),$$

سپس TTP مقدار O_i را محاسبه کرده و با O_i دریافتی از SP_j مقایسه می‌کند. در صورت برابری هر دو مقدار، TTP متقاعد می‌شود که کاربر i قانونی و مجاز است و مقادیر رابطه (۸) را محاسبه می‌کند.

$$BSP_j = h(PSPID_j \| SPID_j \| y),$$
$$E_i = BSP_j \oplus V_i, \quad (۸)$$

سپس TTP، مقدار Z_i را محاسبه کرده و با Z_i دریافتی از SP_j مقایسه می‌کند. اگر هر دو مقدار برابر باشند، TTP متقاعد می‌شود که SP_j با شناسه $SPID_j$ فراهم‌کننده خدمات مورد تأییدی برای کاربر i می‌باشد. بعد از فرآیند احراز هویت کاربر و فراهم‌کننده خدمات، TTP عدد تصادفیِ N_{TTP} را تولید کرده و با استفاده از آن، مقادیر رابطه (۹) را محاسبه کرده و برای SP_j ارسال می‌کند.

$$P_{TTP} = N_{TTP} \oplus PN_i,$$
$$R_{TTP} = N_i \oplus N_{TTP} \oplus h(BSP_j \| N_j), \quad (۹)$$
$$SK_{TTP} = h(N_i \oplus N_{TTP} \oplus N_j),$$
$$Q_{TTP} = h((N_j \oplus N_{TTP}) \| SK_{TTP}),$$
$$V_{TTP} = h((N_i \oplus N_{TTP}) \| SK_{TTP}),$$

هنگامی‌که SP_j مقادیر رابطه (۹) را از TTP دریافت می‌کند، مقادیر رابطه (۱۰) را حساب می‌کند.

$$W_j = h(BSP_j \| N_j), \quad (۱۰)$$
$$SK_j = h(N_i \oplus N_{TTP} \oplus N_j),$$

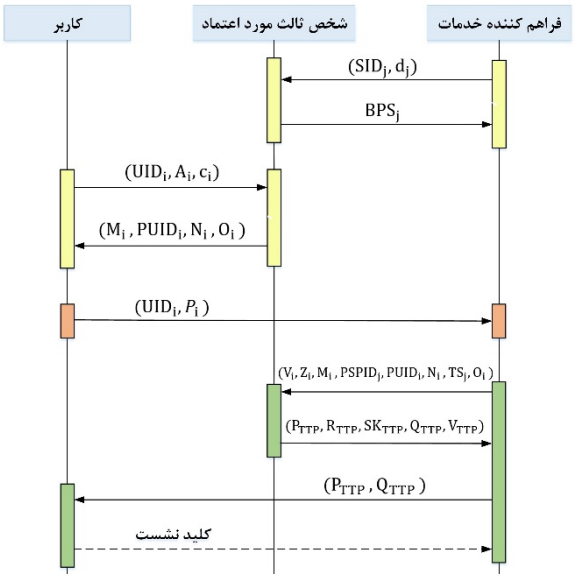
سپس SP_j، مقدار V_{TTP} را محاسبه کرده و با V_{TTP} دریافتی از TTP مقایسه می‌کند. اگر هر دو مقدار برابر باشند، SP_j مقادیر (P_{TTP}, Q_{TTP}) را برای کاربر i ارسال می‌کند.

هنگامی‌که کاربر i مقادیر (P_{TTP}, Q_{TTP}) را از SP_j دریافت می‌کند، مقادیر رابطه (۱۱) را محاسبه می‌کند.

$$L_i = h(D_i \| N_i), \quad (۱۱)$$
$$SK_i = h(N_i \oplus N_{TTP} \oplus N_j),$$

سپس کاربر i، مقدار Q_{TTP} را محاسبه کرده و با Q_{TTP} دریافتی از SP_j مقایسه می‌کند. اگر هر دو مقدار برابر باشند، کاربر از احراز هویت فراهم‌کننده خدمات و شخص ثالث مطمئن شده و کلید نشست که همان SK_i است را برای SP_j ارسال می‌کند.

شکل (۲) خلاصه‌ای از تمامی مراحل مورد نیاز برای انجام فرآیند احراز هویت را نشان می‌دهد. در این شکل، مرحله ثبت‌نام با رنگ زرد، مرحله ورود با رنگ نارنجی و مرحله احراز هویت با رنگ سبز نشان داده شده است.



شکل (۲): دیاگرام ترتیبی مراحل احراز هویت.

۴- تحلیل و ارزیابی

در این بخش نتایج حاصل از پیاده‌سازی روش پیشنهادی مورد بررسی قرار می‌گیرد. نتایج با سه روش امین و همکاران [۱۱]، ژو و همکاران [۱۲] و یو و همکاران [۱۸] مقایسه می‌شود. در شبیه‌سازی از دو نرم‌افزار AVISPA برای سنجش اعتبارسنجی پروتکل و از نرم‌افزار Matlab برای ارزیابی هزینه محاسبه و سرعت ارتباطات استفاده شده است.

۴-۱- تنظیمات شبیه‌سازی

AVISPA[1] ابزاری برای اعتبارسنجی امنیتی پروتکل‌های مختلف است. این ابزار به‌واسطه وجود کتابخانه‌ها و ماژول‌های مختلف، تجزیه و تحلیل‌های مختلف و متعددی را روی پروتکل‌ها برای شناسایی نقاط غیر ایمن آن‌ها اعمال می‌کند. در این ابزار برای سنجش عملکرد پروتکل، نیاز است که ساختار پروتکل به زبان قابل شناخت در محیط با ساختار HLPSL تبدیل گردد. محیط AVISPA توانایی ترجمه و فهم این ساختار را دارد و با اعمال انواع روش‌های سنجش پروتکل، ایمن بودن آن را می‌سنجد. HLPSL یک زبان رسمی سطح بالا، مدولار، مبتنی بر نقش برای مدل‌سازی پروتکل‌های ارتباطی و امنیتی است. ویژگی‌های HLPSL اجازه می‌دهد که یک پروتکل را بدون استفاده از روش های خاص برای ساده‌سازی اولیه، پیاده‌سازی نمود.

این نرم‌افزار دارای ابزارهای OFMC [۱۹] و Cl_Atse [۲۰] به‌عنوان شاخص‌های سنجش میزان امن بودن پروتکل می‌باشد که شاخص OFMC[2] یک بررسی‌کننده مدل در لحظه-همزمان برای یک پروتکل با خصوصیات عملکرد رمزنگاری جبری مهم است و تنها برای پروتکل‌های جعل مؤثر به‌کارگرفته نمی‌شود (به‌عنوان مثال تشخیص سریع حملات) بلکه برای تائید نیز به‌کار می‌رود (اثبات صحیح پروتکل). شاخص Cl_Atse[3] جستجوگر حملات مبتنی بر منطق محدودیتی می‌باشد، همچنین یک سامانه مبتنی بر محدودیت است که راهبرد آن، ترجمه مشخصات پروتکل امنیتی نسبت به مجموعه‌ای از محدودیت‌ها است که می‌تواند به‌طور مؤثر حملاتی که توسط مهاجمین به پروتکل‌ها وارد می‌شود را شناسایی نماید. در جدول (۲) مشخصات محیط آزمایش نشان داده شده است.

جدول (۲): مشخصات محیط آزمایش.

سیستم‌عامل	حافظه اصلی	نوع پردازنده
Windows 10	8 GB	Intel Core i7 3.2 GHZ

۴-۲- تحلیل رسمی و غیررسمی پروتکل پیشنهادی

در این قسمت پروتکل پیشنهادی را از نظر جنبه‌های امنیتی یعنی نیازمندی‌ها و حملات امنیتی به‌صورت رسمی و غیررسمی تحلیل نموده و نیز پروتکل را از نظر جنبه‌های تحلیل کارایی که شامل پارامترهای هزینه، زمان محاسبات و هزینه ارتباطی و ابزارهای اعتبارسنجی OFMC و Cl_Atse می‌باشند، مورد بررسی قرار داده و نتایج آن را در شکل‌های مختلف نمایش می‌دهد. در روش پیشنهادی برای تحلیل امنیتی پروتکل از دو روش غیررسمی و رسمی استفاده می‌شود. در روش غیررسمی، روش پیشنهادی را با توجه به میزان برآورده‌سازی خدمت‌های امنیتی و نیز استحکام در برابر حملات، سنجیده می‌شود و در روش رسمی پروتکل پیشنهادی را با ابزار AVISPA کنترل کرده و امنیت آن مورد بررسی و ارزیابی قرار می‌گیرد.

۴-۲-۱- تحلیل رسمی امنیت پروتکل پیشنهادی (توصیف رسمی پروتکل با استفاده از AVISPA)

در تحلیل امنیتی به روش رسمی میزان امن بودن روش پیشنهادی با ابزار AVISPA مورد ارزیابی قرار می‌گیرد. ابتدا در این بخش پروتکل پیشنهادی با قالب HLPSL به‌صورت مشروح مطرح می‌گردد. در ادامه روش پیشنهادی با سه روش امین و همکاران [۱۱]، ژو و همکاران [۱۲] و یو و همکاران [۱۸] با استفاده از ابزارهای OFMC و Cl_Atse مقایسه می‌شود.

در این شبیه‌سازی میزان امن بودن پروتکل با استفاده از آزمایش‌های متفاوت حمله مورد ارزیابی قرار می‌گیرد. شکل (۶-۳)، میزان امنیت پروتکل پیشنهادی و سه روش امین و همکاران [۱۱]، ژو و همکاران [۱۲] و یو و همکاران [۱۸] را در سنجش توسط شاخص OFMC در ابزار AVISPA نشان می‌دهد.

[1] Automated Validation of Internet Security Protocol and Applications
[2] On-the-Fly Model-Checker
[3] Constraint-Logic-based Attack Searcher

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/Propsed.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.09s
  visitedNodes: 3 nodes
  depth: 6 plies
```

شکل (۳): ارزیابی امنیت پروتکل پیشنهادی در سنجش توسط شاخص OFMC.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/Ref1.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.14s
  visitedNodes: 3 nodes
  depth: 6 plies
```

شکل (۴): ارزیابی امنیت پروتکل پیشنهادی امین و همکاران در سنجش توسط شاخص OFMC.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  UNSAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/Ref2.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.07s
  visitedNodes: 3 nodes
  depth: 5 plies
```

شکل (۵): ارزیابی امنیت پروتکل پیشنهادی ژو و همکاران در سنجش توسط شاخص OFMC.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/Ref3.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.09s
  visitedNodes: 6 nodes
  depth: 9 plies
```

شکل (۶): ارزیابی امنیت پروتکل پیشنهادی یو و همکاران در سنجش توسط شاخص OFMC.

شکل (۷)، (۸)، (۹) و (۱۰) میزان امنیت پروتکل پیشنهادی و سه روش امین و همکاران [۱۱]، ژو و همکاران [۱۲] و یو و همکاران [۱۸] را در سنجش توسط شاخص CL_Atse در ابزار AVISPA نشان می‌دهد.

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/Proposed.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 6 states
  Reachable  : 6 states
  Translation: 0.010 seconds
  Computation: 0.02 seconds
```

شکل (۷): ارزیابی امنیت پروتکل پیشنهادی در سنجش توسط شاخص CL_Atse.

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/Ref1.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 6 states
  Reachable  : 6 states
  Translation: 0.09 seconds
  Computation: 0.04 seconds
```

شکل (۸): ارزیابی امنیت پروتکل پیشنهادی امین و همکاران در سنجش توسط شاخص CL_Atse.

```
SUMMARY
UNSAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/Ref2.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 4 states
  Reachable  : 3 states
  Translation: 0.06 seconds
  Computation: 0.01 seconds
```

شکل (۹): ارزیابی امنیت پروتکل پیشنهادی ژو و همکاران در سنجش توسط شاخص CL_Atse.

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/Ref3.if
GOAL
  As Specified
BACKEND
  CL-AtSe
STATISTICS
  Analysed   : 5 states
  Reachable  : 5 states
  Translation: 0.05 seconds
  Computation: 0.01 seconds
```

شکل (۱۰): ارزیابی امنیت پروتکل پیشنهادی یو و همکاران در سنجش توسط شاخص CL_Atse.

در بخش بعد به تفکیک، به بررسی انواع نیازمندی‌ها و حملات امنیتی پرداخته می‌شود.

۴-۲-۲- تحلیل غیررسمی پروتکل پیشنهادی

در طراحی هر پروتکلی باید یکسری از نیازمندی‌ها و تحلیل‌های امنیتی را در نظر گرفت. در این قسمت پروتکل طراحی‌شده را در مقابل نیازمندی‌های امنیتی و حملات مطرح‌شده مورد تحلیل و بررسی قرار داده و نشان داده شده است که پروتکل پیشنهادی تمام نیازمندی‌های امنیتی ذکرشده را تضمین می‌کند و در برابر تمام حملات ذکرشده مقاوم است.

الف) تضمین نیازمندی‌های امنیتی

به‌منظور استحکام امنیت سامانه، باید در پروتکل‌های احراز هویت، نیازمندی‌های امنیتی مانند احراز هویت متقابل، محرمانگی، کنترل دسترسی و مقیاس‌پذیری تضمین و در نظر گرفته شود، در زیر این نیازمندی‌های امنیتی در پروتکل پیشنهادی بررسی می‌شود.

- **احراز هویت متقابل**

در پروتکل پیشنهادی زمانی که کاربر جهت گرفتن خدمات، تقاضایی را به خدمات‌دهنده ابری ارسال می‌کند، خدمات‌دهنده ابری ابتدا برچسب زمانی درخواست کاربر را مورد بررسی قرار داده و چنانچه منقضی نشده باشد برای تائید احراز هویت درخواست کاربر را به مرکز شخص ثالث ارسال می‌کند و مرکز شخص ثالث نیز پس از بررسی برچسب زمانی و تولید کلید و همچنین تعیین سطح دسترسی کاربر از دوره زمانی نتیجه احراز هویت و همچنین کلید تولیدشده را برای بررسی به خدمات‌دهنده ابری ارسال می‌کند و خدمات‌دهنده ابری نیز پس از استخراج کلید و بررسی مجوز کاربر در ادامه نتیجه مجوز و کلید مربوط به کاربر را برایش ارسال می‌کند. کاربر نیز پس از استخراج کلید و اطمینان از برقراری ارتباط امن با خدمات‌دهنده ابری شروع به ارسال و دریافت خدمات می‌کند. پس با توجه به اینکه احراز هویت در هر دو قسمت کاربر و خدمات‌دهنده ابری به‌صورت کامل انجام می‌شود، نشان می‌دهد که روش پیشنهادی نیازمندی‌های امنیتی احراز هویت متقابل را فراهم می‌کند.

- **محرمانگی**

در روش پیشنهادی از تابع چکیده‌ساز یک‌طرفه h() استفاده می‌شود و همچنین مرکز شخص ثالث برای کلیه پیام‌هایی که قرار است بین کاربر و خدمات‌دهنده ابری و مرکز شخص ثالث جابجا شوند از متغیرهای رمزنگاری و اعداد تصادفی به‌صورت جداگانه استفاده می‌نماید، به‌عنوان مثال کاربر پس از اینکه وارد شبکه شد سریعاً پس از گرفتن شناسه و رمز عبور مقادیرش با متغیر تصادفی bi توسط تابع رمزنگاری چکیده‌ساز یک‌طرفه h() الحاق می‌گردد و برای شخص ثالث ارسال می‌شود. مرکز شخص ثالث نیز پس از دریافت پیام از کاربر مقادیر ارسالی را با استفاده از عدد x که جهت رمزنگاری محاسبات برای کاربر استفاده می‌شود، رمزنگاری نموده و مجدداً پس از انتقال آن‌ها در متغیرهایی، اطلاعاتی را در بانک اطلاعاتی خود در قالب جدول‌های متفاوت یکی برای خود و یکی برای کاربر ذخیره‌سازی می‌نماید. خدمات‌دهنده ابری نیز به همین شیوه ثبت‌نام و به مجموعه وارد می‌شود که این نشان می‌دهد در روش پیشنهادی موضوع محرمانگی به‌صورت کامل مد نظر قرار گرفته شده است.

- **کنترل دسترسی**

در روش پیشنهادی کاربر پس از ثبت‌نام و ورود، سریعاً از طریق مرکز شخص ثالث احراز هویت شده و از طریق دوره زمانی عملکردش بررسی و سطح دسترسی برایش مشخص می‌شود. در نتیجه با توجه به اینکه کاربر فقط به یک سری منابع مقرر دسترسی دارد، نشان می‌دهد روش پیشنهادی از لحاظ نیازمندی امنیتی کنترل دسترسی مقاوم خواهد بود.

- **مقیاس‌پذیری**

روش پیشنهادی طوری طراحی شده که در قسمت مدیریت کاربر، کاربرها به‌راحتی می‌توانند پس از طی مراحل ثبت‌نام و احراز هویت به شبکه وارد شوند و به‌عنوان کاربر جدید، اطلاعات امنیتی خود را در مرکز شخص ثالث ذخیره‌سازی نمایند و خدمات مورد نیازشان را دریافت نمایند. پس با توجه به اینکه پروتکل پیشنهادی توسعه‌پذیر است و اجازه می‌دهد تا کاربر جدیدی درون شبکه اضافه شود و پایدار بماند، می‌توان گفت که روش پیشنهادی نیازمندی امنیتی مقیاس‌پذیری را پوشش می‌دهد. در ادامه، پروتکل پیشنهادی با سه پروتکل امین و همکاران [۱۱]، ژو و همکاران [۱۲] و یو و همکاران [۱۸] از نظر نیازمندی‌های امنیتی در جدول (۳) مقایسه خواهد شد.

جدول (۳): نیازمندی‌های امنیتی اجراشده برای پروتکل‌ها.

	مقیاس پذیری	دسترس پذیری	محرمانگی	احراز هویت متقابل
روش پیشنهادی	✓	✓	✓	✓
امین و همکاران [۱۱]	×	×	✓	✓
ژو و همکاران [۱۲]	×	×	×	✓
یو و همکاران [۱۸]	✓	×	✓	✓

ب) استحکام در برابر حملات امنیتی

در این بخش به بررسی انواع حملات و همچنین مقاومت پروتکل پیشنهادی در برابر حملات استراق سمع، تکرار، حدس زدن رمز عبور به‌صورت برون‌خط، حمله داخلی مجاز شده (امتیازدار)، جعل هویت کاربر، انکار خدمات (DoS) و حمله مرد میانی پرداخته می‌شود. در جدول (۴) پروتکل پیشنهادی با سه پروتکل امین و همکاران [۱۱]، ژو و همکاران [۱۲] و یو و همکاران [۱۸] از نظر مقاومت در برابر حملات امنیتی مقایسه می‌شود.

جدول (۴): مقاومت در برابر حملات امنیتی در پروتکل‌های مختلف.

	حمله مرد میانی	انکار خدمات(DoS)	حمله جعل هویت	حمله داخلی مجاز شده	رمز عبور حدس زدن	حمله تکرار	حمله استراق سمع
روش پیشنهادی	✓	✓	✓	✓	✓	✓	✓
امین و همکاران[۱۱]	×	×	✓	✓	✓	✓	✓
ژو و همکاران [۱۲]	×	×	×	×	×	✓	✓
یو و همکاران [۱۸]	✓	✓	✓	×	✓	✓	✓

همان‌طور که در جدول (۴) نشان داده شده است، روش پیشنهادی در برابر تمامی حملات مقاوم است، در حالی‌که سایر روش‌ها حداقل در برابر یکی از حملات آسیب‌پذیر هستند.

۴-۳- تحلیل کارایی پروتکل پیشنهادی

این بخش روش پیشنهادی را با استفاده از معیارهای ارزیابی که شامل معیار زمان محاسبات و معیار هزینه ارتباطی می‌باشد، مورد بررسی قرار داده و نتایج آن را در جداول مختلف نمایش می‌دهد. معیار زمان محاسبات، که مدت زمان محاسبات انجام‌شده در مراحل مختلف پروتکل می‌باشد. این زمان از رابطه (۱۲) حاصل می‌شود، که به ترتیب T_h زمان انجام رمزنگاری چکیده‌ساز یک‌طرفه و T_E زمان محاسبات نمایی است.

$$CT = T_h + T_E \qquad (۱۲)$$

معیار هزینه ارتباطی، تعداد بیت‌های مبادله شده در طول اجرای پروتکل بین اجزا است. این زمان از رابطه (۱۳) حاصل می‌شود، که به ترتیب CCL هزینه ارتباطی در مرحله ورود کاربر و CCA هزینه ارتباطی در مرحله احراز هویت است.

$$CCT = CCL + CCA \qquad (۱۳)$$

۴-۳-۱- ارزیابی هزینه محاسباتی

در این شبیه‌سازی هزینه محاسباتی پروتکل پیشنهادی ارزیابی و با روش‌های مرجع مقایسه می‌گردد. جدول (۵) هزینه محاسباتی هر روش را برای کاربر، فراهم‌کننده خدمات و شخص ثالث نشان می‌دهد. همان‌طور که در شکل نشان داده شده است، روش پیشنهادی کمترین تعداد علمیات درهم‌سازی را در مقایسه با روش‌های دیگر دارد.

جدول (۵): ارزیابی هزینه محاسباتی بر حسب عملیات.

روش	کاربر	فراهم‌کننده خدمات	شخص ثالث	مجموع
پیشنهادی	12 T_h	4 T_h	12 T_h	28 T_h
امین و همکاران [۱۱]	12 T_h	4 T_h	14 T_h	30 T_h
ژو و همکاران [۱۲]	12 T_h	6 T_h	18 T_h	36 T_h
یو و همکاران [۱۸]	12 T_h	6 T_h	16 T_h	34 T_h

جدول (۶) مجموع هزینه زمان محاسبات را در روش‌های مختلف بر حسب ثانیه را برای دو حالت مختلف نشان می‌دهد. در حالت اول هزینه تابع درهم‌سازی برابر با ۰,۰۰۵۱۷ و در حالت دوم هزینه تابع درهم‌سازی برابر با ۰,۰۰۰۰۳۲۸ در نظر گرفته شده است.

جدول (۶): ارزیابی هزینه محاسباتی بر حسب ثانیه.

روش	هزینه مجموع حالت ۱	هزینه مجموع حالت ۲
پیشنهادی	0.1539 ms	0.00191 ms
امین و همکاران [۱۱]	0.1551 ms	0.00098 ms
ژو و همکاران [۱۲]	0.1861 ms	0.00118 ms
یو و همکاران [۱۸]	0.1758 ms	0.00111 ms

با توجه به جدول (۶)، زمان محاسبات در روش پیشنهادی نسبت به روش‌های دیگر برای هر دو حالت کاهش یافته است.

۴-۳-۲- ارزیابی هزینه ارتباطی

در این شبیه‌سازی هزینه ارتباطی با تغییر تعداد کاربرها محاسبه می‌گردد. نکته مهم در این ارزیابی این است که با افزایش تعداد کاربرها صفی از درخواست احراز هویت شکل خواهد گرفت. جدول (۷) میانگین هزینه ارتباطی را به‌صورت کلی نشان می‌دهد.

جدول (۷): ارزیابی هزینه ارتباطی.

روش	CCL	CCA	مجموع
پیشنهادی	2198 bit	765 bit	2963 bit
امین و همکاران [۱۱]	2263 bit	788 bit	3051 bit
ژو و همکاران [۱۲]	2446 bit	812 bit	3258 bit
یو و همکاران [۱۸]	2385 bit	799 bit	3184 bit

جدول (۷) نشان می‌دهد که پروتکل پیشنهادی هزینه ارتباطی کمتری نسبت به روش‌های پیشین دارد.

۵- نتیجه‌گیری

در این مقاله روشی برای احراز هویت و تعیین سطح دسترسی کاربرهای مبتنی بر اینترنت اشیا در محیط ابر ارائه شد. در چارچوب پیشنهادی مقاله سه نوع ارتباط امن و مهم شامل ارتباط بین کاربرها و مرکز شخص ثالث، ارتباط بین خدمات‌دهنده‌های ابری و مرکز شخص ثالث و ارتباط بین کاربرها و خدمات‌دهنده‌های ابری وجود دارد. به‌طور مشخص هر نوع ارتباط باید با تائید مرکز شخص ثالث انجام شود. در روش پیشنهادی مرکز شخص ثالث وظیفه کنترل و نظارت بر امنیت خدمات و عملکرد کاربرها در ابر شامل ثبت‌نام، احراز هویت و برقراری ارتباط امن بین کاربرها و خدمات‌دهنده‌ها را به عهده دارد. نتایج به‌دست‌آمده نشان دادند که روش پیشنهادی در ارزیابی رسمی توسط دو ابزار OFMC و Cl-AtSe ایمن است و به‌علاوه نسبت به روش‌های پیشین هزینه محاسباتی کمتر و هزینه ارتباطی کمتری دارد. مباحث امنیتی مربوط به پایگاه داده در ارائه‌دهنده ابر در این مطالعه مورد توجه قرار نگرفته است. بنابراین، یکی از کارهای آینده، آزمایش سامانه احراز هویت تحت تهدید پایگاه داده می‌باشد.

۶- مراجع

[1] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, "Authenticated key agreement scheme for fog-driven IoT healthcare system," Wireless Networks, vol. 25, no. 8, pp. 4737-4750, 2019.

[2] A. A. Alamr, F. Kausar, J. Kim, and C. Seo, "A secure ECC-based RFID mutual authentication protocol for internet of things," The Journal of Supercomputing, vol. 74, no. 9, pp. 4281-4294, 2018.

[3] S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers," Pervasive and Mobile Computing, vol. 24, pp. 210-223, 2015.

[4] T.-Y. Wu, Z. Lee, M. S. Obaidat, S. Kumari, S. Kumar, and C.-M. Chen, "An authenticated key exchange protocol for multi-server architecture in 5G networks," IEEE Access, vol. 8, pp. 28096-28108, 2020.

[5] F. Wu, X. Li, L. Xu, A. K. Sangaiah, and J. J. Rodrigues, "Authentication protocol for distributed cloud computing: An explanation of the security situations for Internet-of-Things-enabled devices," IEEE Consumer Electronics Magazine, vol. 7, no. 6, pp. 38-44, 2018.

[6] Y. Yu, L. Hu, and J. Chu, "A Secure Authentication and Key Agreement Scheme for IoT-Based Cloud Computing Environment," Symmetry, vol. 12, no. 1, p. 150, 2020.

[7] D. He, S. Zeadally, N. Kumar, and W. Wu, "Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures," IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 2052-2064, 2016.

[8] H. Khemissa and D. Tandjaoui, "A novel lightweight authentication scheme for heterogeneous wireless sensor networks in the context of Internet of Things," in 2016 Wireless Telecommunications Symposium (WTS), 2016, pp. 1-6: IEEE.

[9] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," Ad Hoc Networks, vol. 20, pp. 96-112, 2014.

[10] R. Amin and G. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," Ad Hoc Networks, vol. 36, pp. 58-80, 2016.

[11] R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment," Future Generation Computer Systems, vol. 78, pp. 1005-1019, 2018.

[12] K. Xue, P. Hong, and C. Ma, "A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture," Journal of Computer and System Sciences, vol. 80, no. 1, pp. 195-206, 2014.

[13] Y. Feng, W. Wang, Y. Weng, and H. Zhang, "A replay-attack resistant authentication scheme for the internet of things," in 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), IEEE, vol. 1, pp. 541-547, 2017.

[14] T. Limbasiya and A. Karati, "Cryptanalysis and improvement of a mutual user authentication scheme for the Internet of Things," in 2018 International Conference on Information Networking (ICOIN), IEEE, pp. 168-173, 2018.

[15] V. Kumar, M. Ahmad, D. Mishra, S. Kumari, and M. K. Khan, "RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing," Vehicular Communications, vol. 22, p. 100213, 2020.

[16] L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance," Future Generation Computer Systems, vol. 91, pp. 244-251, 2019.

[17] M. Wazid, A. K. Das ,V. Bhat, and A. V. Vasilakos, "LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment," Journal of Network and Computer Applications, vol. 150, p. 102496, 2020.

[18] S. Yu, K. Park, and Y. Park, "A secure lightweight three-factor authentication scheme for IoT in cloud computing environment," Sensors, vol. 19, no. 16, p. 3598, 2019.

[19] D. Basin, S. Mödersheim, and L. Vigano, "OFMC: A symbolic model checker for security protocols," International Journal of Information Security, vol .4, no. 3, pp. 181-208, 2005.

[20] M. Turuani, "The CL-Atse protocol analyser," in International Conference on Rewriting Techniques and Applications, Springer, pp. 277-286, 2006.

نشریه علمی "پدافند الکترونیکی و سایبری"
سال نهم، شماره ۲، تابستان ۱۴۰۰، ص ۲۸-۱۷

*Corresponding Author E-mail: a.shahidinejad@qom-iau.ac.ir