Journal of the Nivar Vol. 47, No. 120-121, Spring and Summer 2023, P. 181-197

Homepage: https://nivar.irimo.ir (Research Article)

BSAMS: Blockchain-Based Secure Authentication Scheme in Meteorological Systems

Salami, Y. [1] ✉ | Hosseine, S.R.[2]

1. **Corresponding Author**, Department of Computer and Information Technology Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran. E-mail: yashar.salami@gmail.com

2. Department of Computer Engineering University College of Daneshvaran Tabriz, Iran. E-mail: rozalweb@gmail.com

(Received: 9 Jun 2023, Revised: 6 Jul 2023, Accepted: 19 Sep 2023, Published online: 19 Sep 2023)

Abstract

The security of communication between Internet of Things devices is a big concern in this field, and with the increase in the number of devices and users, the current architecture and communication protocols cannot adequately respond to the system's needs, such as authentication and access authorization. One of the important solutions to this problem is using distributed and decentralized networks such as blockchain. So far, various blockchain-based authentication and key agreement protocols have been presented in the Internet of Things and similar environments. However, a secure authentication scheme has not been proposed for meteorological systems. This paper proposes a secure authentication scheme based on the blockchain network for meteorological systems resistant to various attacks. The Security of the proposed project against formal and informal attacks is evaluated, and the analysis results show that Securityrity of the proposed scheme resists active and passive attacks. In the following, the proposed scheme is evaluated in terms of computational costs, and the evaluation results show that the proposed scheme is increasing compared to similar schemes due to the focus on computational security.

Keywords: Blockchain, Meteorological, Security, Authentication, Access contro.

Cite this article: Salami, Y., & hosseini, S. (2023). BSAMS: Blockchain-Based Secure Authentication Scheme in Meteorological Systems. Journal of the Nivar, Vol. 47, No. 120-121. 181-197. DOI: https://doi.org/10.30467/nivar.2023.415722.1260

Publisher: Iran Meteorological Organization
DOI: https://doi.org/10.30467/nivar.2023.415722.1260

Print ISSN: 1735-0565
Online ISSN: 2645-3347

نیوار
دوره ۴۷، شماره ۱۲۰– ۱۲۱، بهار و تابستان ۱۴۰۲، صفحه ۱۸۱– ۱۹۷
نشانی اینترنتی مجله: https://nivar.irimo.ir
(مقاله پژوهشی)

طرح احراز هویت ایمن مبتنی بر بلاکچین در سیستم‌های هواشناسی

یاشار سلامی[۱] ✉ | **سیدرضا حسینی**[۲]

۱. **نویسنده مسئول**، دانشجوی دکتری گروه مهندسی کامپیوتر و فناوری اطلاعات، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران. رایانامه: yashar.salami@gmail.com

۲. دانشجوی کارشناسی ارشد مهندسی کانپیوتر گرایش نرم افزار موسسه آموزش عالی دانش وران تبریز ، تبریز، ایران. رایانامه: rozalweb@gmail.com

(دریافت: ۱۴۰۲/۰۳/۱۹، بازنگری: ۱۴۰۲/۰۴/۱۵، پذیرش: ۱۴۰۲/۰۶/۲۸، انتشار آنلاین: ۱۴۰۲/۰۶/۲۸)

چکیده

امنیت ارتباطات بین دستگاه‌های اینترنت اشیا یک نگرانی بزرگ در این زمینه است و با افزایش تعداد دستگاه‌ها و کاربران، معماری فعلی و پروتکل‌های ارتباطی نمی‌توانند به نیازهای سیستم مانند احراز هویت، مجوز دسترسی پاسخ کافی بدهند. یکی از راه حل های مهم این مسئله استفاده از شبکه‌های توزیع شده و غیرمتمرکز مانند بلاکچین است. تاکنون پروتکلهای احراز هویت و توافق کلید مختلفی مبتنی بر بلاکچین در اینترنت اشیا و سایر محیط ها مشابه ارائه شده است با این حال طرح احراز هویت امنی برای سیستم‌های هواشناسی پیشنهاد نشده است .در این مقاله، ما طرح احراز هویت ایمن مبتنی بر شبکه بلاکچین را برای سیستم‌های هواشناسی پیشنهاد میدهیم که در برابر حملات مختلف مقاوم است.. امنیت طرح پیشنهادی در مقابل حملات به صورت رسمی و غیر رسمی، مورد ارزیابی قرار گرفته و نتایج تجزیه و تحلیل امنیتی نشان می‌دهد که امنیت طرح پیشنهادی در مقابل حملات اکتیو و پسیو مقاوم است. در ادامه طرح پیشنهادی از نظر هزینه‌های پردازشی مورد ارزیابی قرار گرفته که نتایج ارزیابی طرح پیشنهادی نشان می‌دهد طرح پیشنهادی نسبت به طرح‌های مشابه به دلیل تمرکز روی امنیت هزینه پردازشی رو به افزایش است.

کلمات کلیدی: بلاکچین،امنیت، هواشناسی ،احراز هویت ، کنترل دسترسی.

۱. مقدمه

اینترنت اشیا مبحثی پیرامون گسترش قدرت اینترنت به مواردی فراتر از کامپیوترها و گوشی‌های هوشمند و در واقع، به طیف وسیعی از چیزها (اشیا)، فرایندها و محیط است. ایده اصلی این مفهوم، حضور فراگیر انواع اشیاء در اطراف ما است [2] ,[1]، از جمله تگ‌هایRFID ، سنسورها، تلفن‌های همراه و غیره که از طریق طرح‌های آدرس‌دهی منحصربه‌فرد قادر هستند با برقراری ارتباط با یکدیگر و همکاری برای دستیابی به اهداف مشترک هماهنگ شوند [3]. به عبارتی این مفهوم را در قالب دنیایی که در آن هر چیز و هر اشیای، دارای هویت دیجیتال باشد و کامپیوترها آن‌ها را کنترل و مدیریت نمایند، مطرح نمود. امروز حس‌گرهای موجود در ایستگاه‌های خودکار نوعی از اینترنت اشیا محسوب می‌شوند. امنیت و محرمانه بودن،مسائل مهمی برای کاربردهای اینترنت اشیا بوده و همچنان با چالش های بزرگی مواجه است[4]. مهم ترین مشکل مرتبط با امنیت در اینترنت اشیاء ، بحث احراز هویت و جامعیت داده‌ها است [5] . از آنجا که احراز هویت معمولاً نیازمند وجود سرورها و زیرساخت های مناسب برای تبادل پیام میان اجزاء مختلف است ، تأمین آن در اینترنت اشیاء کار دشواری است. همچنین با افزایش تعداد دستگاه‌ها و کاربران، معماری کنونی سیستم هواشناسی و پروتکل‌های ارتباطی موجود نمی‌توانند به نیازهای

استناد: مزیدی, احمد, محمدی راوری, فروغ, & بهزادی شهربابک, زهرا. (۱۴۰۲). ارزیابی وضعیت خشکسالی شهر کرمان با استفاده از شاخص‌های خشکسالی و ارتباط آن با تغییرات پوشش گیاهی منطقه، مجله نیوار، دوره ۴۷، شماره ۱۲۰– ۱۲۱، ۱۸۱– ۱۹۷. DOI: https://doi.org/10.30467/nivar.2023.394900.1244

ناشر: سازمان هواشناسی کشور.
DOI: https://doi.org/10.30467/nivar.2023.394900.1244

اساسی احراز هویت و مجوز دسترسی پاسخ بدهند. یکی از راه حل های موجود، استفاده از بلاکچین می‌باشد. این فنّاوری تجهیزات موجود را قادر می‌سازد که از اتکا به یک سیستم متمرکز جهت احراز هویت و کنترل دسترسی بی‌نیاز شوند و با ایجاد یک شبکه امن، امکان برقراری ارتباط ایمن بین تجهیزات مختلف هواشناسی را فراهم می‌کند.

۱-۱. سازمان مقاله

سازمان مقاله به شرح زیر است : بخش دوم مدل شبکه طرح پیشنهادی و تعریف مسئله را بیان می‌کند. در بخش سوم اطلاعات کلی شبکه بلاکچین و بخش چهارم سوابق تحقیق را ارائه می‌دهد. در بخش پنجم طرح پیشنهادی بیان‌شده است. بخش ششم تجزیه تحلیل امنیتی طرح پیشنهادی را شرح می‌دهد. بخش هفتم به تحلیل ارزیابی طرح پیشنهادی می‌پردازد و در نهایت در بخش هفتم نتیجه‌گیری ارائه می‌شود.

۲. مدل شبکه

این بخش مدل شبکه طرح پیشنهادی و بیان مسئله را شرح می‌دهد.

این مقاله از یک مدل شبکه برای تعریف ارتباطات بین ایستگاه هواشناسی و شبکه بلاکچین استفاده شده است که شکل ۱ ارتباط مدل شبکه‌ای را نشان می‌دهد. مدل شبکه پیشنهادی از اجزای زیر تشکیل شده است.

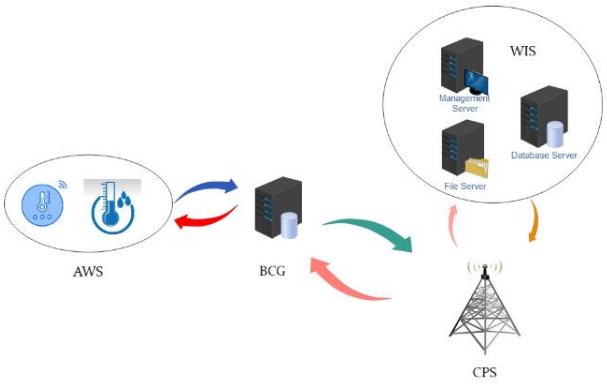
AWS: ایستگاه هواشناسی خودکار است که از مجموعه حس‌گرها برای اعلان وضعیت آب و هوا تشکیل شد است.

BCG: دروازه شبکه بلاکچین است که به عنوان یک واسط بین ایستگاه هواشناسی و CPS است. این دروازه‌ها واجد شرایط بودن CPS (مجوزها و احراز هویت) برای استفاده از اطلاعات و منابع ایستگاه‌های هواشناسی را طبق سیاست‌های ایستگاه‌ها را ارزیابی می‌کنند.

CPS: یک سیستم کنترل پروسه است که وظیفه آن انجام پردازش های لازم بر روی داده‌های دریافتی از AWS هست.

WIS: سیستم هواشناسی جهانی است که برای تبادل اطلاعات و اشتراک گذاری اطلاعات هواشناسی بین سازمان‌ها و مرکز مختلف هواشناسی استفاده می‌شود.

ارتباط اجزای مدل شبکه به این صورت است که داده‌های خام از شرایط جوی توسط حس‌گرها AWS جمع آوری می‌شود و برای پردازش به CPS ارسال می‌شود.CPS بعد از انجام پردازش روی داده‌ها خام ، داده‌های پردازش شده را برای استفاده به WIS ارسال می‌کند. با این حال این امکان وجود داد که داده‌های ارسالی بین AWS و CPS توسط شخص سومی مورد حمله قرار بگیرد به همین دلیل برای جلوگیری از حملات اکتیو و پسیو نیاز است که قبل از ارسال داده هویت دو طرف ارتباط توسط BCG تائید شود احراز هویت متقابل بین طرفین ارتباط در محیط هواشناسی یکی از چالش های مهم در این حوزه است.



شکل ۱ . ساختار شبکه طرح پیشنهادی

۲-۱. بیان مسئله

در شبکه‌های بیسیم، ارتباط بین دستگاه‌ها به صورت بی‌سیم و از طریق امواج رادیویی انجام می‌شود. با توجه به اینکه شبکه‌های بیسیم مستعد حملات اکتیو و پسیو هستند این امکان وجود دارد که هنگام ارتباط بین دو طرف، یک فرد یا گروهی در میان قرار گرفته و ترافیک ارتباط را میانبر کرده و اطلاعات را آزار داده یا دزدیده می‌کند. در شبکه بیسیم این امکان وجوددارد که حمله کنند می‌تواند به طور فیزیکی به امواج رادیویی دسترسی داشته باشد و بتواند آن‌ها را مانیتور کند و مداخله کند. با در نظر گرفتن این مسئله این امکان وجود دارد که حمله کنند بین AWS و CPS قرار گیرد و داده‌های ارسالی بین طرفین ارتباط را دست‌کاری یا شنود کند به همین دلیل ایجاد یک کانال امن

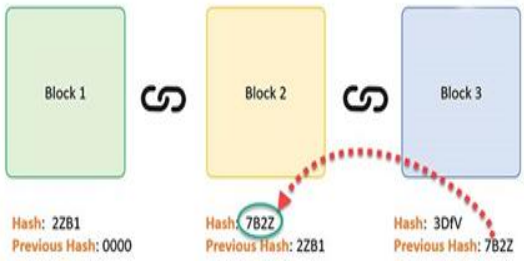
باقابلیت احراز هویت با کمک شبکه بلاکچین یک ضرورت مهم در این حوزه است.

۳. شبکه بلاکچین

این بخش اطلاعاتی کلی از نحوی عملکرد شبکه بلاکچین را ارائه می‌دهد.

شبکه بلاکچین یک پایگاه داده یا به عبارتی یک سیستم ثبت اطلاعات و گزارش می‌باشد و می‌توان گفت بلاکچین یک تکنولوژی نوظهور در قرن حاضر است [6]. یکی از تفاوت های اصلی بلاکچین با دیگر سیستم‌های ذخیره اطلاعات این است که اطلاعات ذخیره شده روی سیستم بلاکچین، میان همه اعضای شبکه به اشتراک گذاشته می‌شوند و با استفاده از رمزنگاری۵ امکان حذف و دست‌کاری اطلاعات ثبت شده تقریباً غیرممکن می‌شود[7]. به دلیل این که اطلاعات در تکنولوژی بلاکچین داخل یک سری بلوک‌هایی است که این بلاک‌ها زنجیره‌وار به یکدیگر متصل هستند از این رو این تکنولوژی بلاکچین نامیده شده است.هر بلاک شامل ۳ بخش اساسی می‌شود:

- اطلاعات: اطلاعات بلاک که شامل تراکنش‌های انجام شده در بلاک است.
- هش: رشته‌ای متنی است که از یک تابع ریاضی خاص تولید شده و کاربرد آن جلوگیری از تقلب در سیستم است
- هش بلاک قبلی: هشِ بلاک قبلی در اصطلاح زنجیره‌ی بلاکچین نامیده می‌شود. از آنجایی که بلاک جدید، هش بلاک قبلی را دربردارد، بلاک‌های بلاکچین بر اساس یکدیگر بنا می‌شوند. بدون این مؤلفه، هیچ ارتباط و گاه‌شماری بین بلاک‌ها شکل نمی‌گیرد. شکل ۲ ساختار بلاک‌ها را در شبکه بلاکچین نشان می‌دهد.



شکل ۲. ساختار بلاک‌ها در بلاکچین.

هر کدام از این بلاک‌ها چیزی به نام هش دارند. یک هش رشته‌ای متنی است که از یک تابع ریاضی خاص تولید شده و کاربرد آن جلوگیری از تقلب در سیستم است. هش یک داده یا ورودی، همیشه ثابت است. استفاده از راهکار هش باعث می‌شود تا از تقلب و تغییر اطلاعات ثبت‌شده روی بلاکچین جلوگیری به عمل آید.

در بلاکچین، بلاک‌ها علاوه بر دارا بودن هش مربوط به خودشان،حاوی هش بلاک قبلی هم هستند.کوچک‌ترین تغییر در اطلاعات یک بلاک، هش آن را به طور کلی تغییر می‌دهد و بلاکچین را غیر معتبر می‌سازد. اگر فردی قصد تغییر داده‌های ذخیره‌شده در یک بلاک از سیستم کلی را داشته باشد، باید هش بلاک قبلی را هم تغییر دهد [8]. به بیان ساده‌تر، باید هش تمام بلاک‌های قبلی را تا اولین بلاک ساخته‌شده در زنجیره تغییر دهد که این روند شدنی نیست و هیچ‌وقت اطلاعات داخل بلاکچین تغییر نخواهد کرد. همچنین در یک شبکه بلاکچین، همه اعضای شبکه در فرآیند تائید اطلاعات شرکت می‌کنند و نقش جایگزین شخص ثالث قابل اعتماد در سیستم را ایفا می‌کنند. دست‌کاری اطلاعات به دلیل نظارت عمومی بر اطلاعات بسیار دشوار خواهد بود[9]. با این وجود، تکنولوژی بلاکچین فقط به یک شکل واحد ارائه نمی‌شود و انواع مختلفی دارد که هر یک تفاوت‌هایی با نسخه‌ی اصلی دارند. در طول چند سال گذشته، بلاکچین ها بر اساس ساختار و پیکربندی خود، به صورت‌های مختلفی تکامل یافته‌اند. محتوای ذخیره شده در بلاکچین و فعالیت مشارکت کنندگان، با توجه به پیکربندی و اهداف تجاری آن، قابل کنترل است[10].

٤. سوابق تحقیق

این بخش،سوابق تحقیق را مورد بررسی قرار می‌دهد و در انتهای بخش جدول۱ مقایسه‌ای بین سوابق انجام شده را با ذکر نقاط ضعف‌های امنیتی را ارائه می‌کند.

در سال ۲۰۱۶، اُوادا و همکاران یک چارچوب جدید کنترل دسترسی مبتنی بر بلاکچین برای اینترنت اشیا ارائه دادند. ایده اصلی طراحی سیستمی برای حفظ حریم خصوصی و امنیت به صورت توزیع شده بود[11]. مشکلی که در این طراح وجود دارد، هزینه محاسباتی بالا برای اعضای شبکه است. در سال ۲۰۱۶،هاشمی و همکاران. در اجلاس بین‌المللی IEEE در مورد طراحی و پیاده سازی اینترنت اشیا یک معماری چند لایه مبتنی بر بلاکچین را برای به اشتراک گذاشتن داده‌های دستگاه‌های اینترنت اشیا با سازمان‌ها و افراد پیشنهاد کردند. معماری پیشنهادی دارای سه جزء اصلی است که عبارت‌اند از: پروتکل مدیریت داده، سیستم ذخیره داده و سرویس پیام. پروتکل مدیریت داده چارچوبی را برای مالک داده، درخواست کننده یا منبع داده فراهم می‌کند تا با یکدیگر ارتباط برقرار کنند. سیستم پیام رسانی برای افزایش مقیاس پذیری شبکه بر اساس مدل انتشار/اشتراک استفاده می‌شود[12]. در نهایت، سیستم ذخیره داده از یک بلاکچین برای ذخیره داده‌ها به صورت خصوصی استفاده می‌کند. با توجه به اینکه در این معماری ، از بلاکچین برای ذخیره داده‌های کاربر استفاده می‌شود، پهنای باند زیادی برای ذخیره داده‌ها در بلاکچین توزیع شده مصرف می‌کند. در سال ۲۰۱۶، کریستیدیس و همکاران شرح مفصلی از نحوه عملکرد بلاکچین و قراردادهای هوشمند، شناسایی مزایا و معایبی که معرفی آنها برای یک سیستم به ارمغان می‌آورد و روش‌هایی را که می‌توان از زنجیره‌های بلوکی و اینترنت اشیا با هم استفاده کرد، مورد بررسی قرار داده‌اند[13]. البته روش پیشنهادی آنها دارای معایبی می‌باشد، به عنوان مثال، از یک طرح لیست سفید برای لغو مکانیسم‌های اجماع۸ در شبکه‌های خصوصی استفاده شده است و باعث افزایش خطرات امنیتی سیستم شده است. در سال ۲۰۱۷، دوری و همکاران روشی را برای فرآیند تولید بلوک و اجماع پیشنهاد کردند که بر اساس محدودیت تعداد بلوک‌های تولید شده در واحد زمان در هر گره است. دوری و همکاران ادعا کرده‌اند که روش پیشنهادی مقیاس پذیر است و بار محاسباتی متناسبی را برای اعضای شبکه فراهم می‌کند[14]. در این طرح، ماینرها عضو شبکه هستند و تعداد و عضویت آنها بر اساس چند پارامتر تغییر می‌کند. اما آنها مفهوم الگوریتم اثبات کار را برای سرعت بخشیدن به کارایی تراکنش‌ها حذف می‌کنند، که خطرات امنیتی سیستم را افزایش می‌دهد. در سال ۲۰۱۷، اوزیلماز و همکاران تلاش کرده‌اند دستگاه‌های اینترنت اشیا کم مصرف را در یک زیرساخت مبتنی بر بلاکچین ادغام کنند[15]. اما این سیستم بر روی بلاکچین اتریوم، که برای دستگاه‌های اینترنت اشیا اضافه بار است، پیاده سازی شده است و توان عملیاتی پایین بلاکچین اتریوم نمی‌تواند خواسته‌های سیستم اینترنت اشیا را برآورده کند. در سال ۲۰۱۸، نوو و همکاران. معماری بر اساس بلاکچین برای مدیریت دسترسی مقیاس پذیر در اینترنت اشیا ارائه دادند[16]. آنها با کاهش توزیع، محاسبات را متناسب با منابع دستگاه‌ها و شبکه بلاکچین را از شبکه عمومی جدا کردند و با استفاده از هاب های مدیریتی با دستگاه‌ها ارتباط را برقرار کردند. این راه حل باعث افزایش عملکرد و کاهش توزیع می‌شود. در مقایسه با طراحی اُوادا و همکاران، قدرت محاسباتی دستگاه‌ها را ارتقا می‌دهد و البته احتمال حملات انکار سرویس توزیع شده را افزایش می‌یابد. در پروتکل نوو ، ماینرها نمی‌توانند عضوی از شبکه باشند که فقط با شبکه بلاکچین همکاری می‌کنند. بار محاسباتی بالا از فرآیند تولید بلوک حاصل می‌شود. با استفاده از فرآیند تولید بلوک سبک تر، می‌توانیم به طور مؤثر از شبکه بلاکچین در اینترنت اشیا (اینترنت اشیا) استفاده کنیم. در سال ۲۰۱۸، دی پیترو و همکاران [17]یک مدل اعتماد توزیع‌شده برای اینترنت اشیا را ارائه دادند که آنها را برای ایجاد اعتماد سرتاسر بین دستگاه‌های اینترنت اشیا بدون هیچ شخص ثالثی ایجاد می‌کند.البته متأسفانه این مدل فقط فناوری بلاکچین را در سیستم اینترنت اشیا اعمال می‌کند و پیاده‌سازی دقیقی را ارائه نمی‌دهد. در سال ۲۰۱۸، حامی و همکاران[18]. سیستم حباب‌های اعتماد را با هدف ارائه مناطق مجازی امن برای احراز هویت دستگاه‌های متصل در محیط‌های اینترنت اشیا به صورت ایمن ارائه دادند. این رویکرد مبتنی بر بلاکچین عمومی است. بنابراین، از ویژگی‌های امنیتی آن استفاده می‌شود و این ویژگی

را دارد که در طیف گسترده‌ای از زمینه‌های اینترنت اشیا اعمال شود. علاوه بر این، نتایج ارزیابی کارایی، توانایی در برآوردن الزامات امنیتی اینترنت اشیاء و هزینه پایین آن را ثابت کرد. این رویکرد از سازگاری با برنامه‌های بلادرنگ رنج می‌برد، زیرا اعتبارسنجی پیام‌های ارسالی به زمان مورد نیاز اجماع بستگی دارد که تقریباً ۱۴ ثانیه طول می‌کشد. در سال ۲۰۱۸، چا و همکاران[19] یک پروتکل احراز هویت جدید مبتنی بر بلاکچین برای مدیریت اشتراک و دسترسی به اطلاعات دستگاه اینترنت اشیا به عنوان یک نگرش توزیع شده پیشنهاد کردند. در این پروتکل، سه موجودیت اصلی وجود دارد. دستگاه، کاربر و دروازه متصل به بلاکچین (BCG) . در این مدل هر کاربر به شبکه بلاکچین می پیوندد و جفت کلید عمومی و خصوصی خود را ثبت می‌کند. BCG ها و مدیر دستگاه‌ها قرارداد هوشمند۱۱خود را در شبکه بلاکچین مستقر می‌کنند. فرآیندهای احراز هویت و مدیریت سیاست های دسترسی توسط قراردادهای هوشمند انجام می‌شود. با تجزیه و تحلیل امنیتی پروتکل توسط آقای یاوری و همکاران اثبات شد پروتکل در مقابل حملات امنیتی دارای ضعف می‌باشد و چهار حمله افشای مخفی ،حمله تکرار ،قابلیت ردیابی،و استفاده مجدد از توکن را می‌توان بر روی پروتکل انجام داد. در سال ۲۰۲۰ رستم پور و همکاران[20]. طرح احراز هویت و توافق کلید نوینی برای دستگاه‌های اینترنت اشیاء مبتنی بر رمزنگاری منحنی بیضوی ارائه دادند. اما به دلیل محاسبات اشتباه طرفین ارتباط(دستگاه و خدمات دهنده) کلیدهای نشست تولید شده با هم برابر نخواهند شد و ارتباط بین طرفین برقرار نمی‌شود. همچنین به دلیل استفاده نکردن از مهرهای زمانی در برخی از مراحل ارتباط، مهاجم می‌تواند پیام‌های تکراری را برای طرفین ارسال کند و باعث اختلال در عملکرد دستگاه و خدمات دهنده بشود. در سال ۲۰۲۰، یاوری و همکاران [21] پروتکل احراز هویت مبتنی بر بلاکچین بهبودیافته (IBCbAP) را ارائه دادند. آنها ادعا می‌کنند با استفاده از تابع HMAC به جای امضای پیشنهادی چا و همکاران، نقاط ضعف پروتکل چا و همکاران را بهبود می‌بخشند. همچنین به دلیل سرعت بیشتر و مصرف حافظه کم تر در رمزگذاری ECDLP نسبت به RSA در پروتکل پیشنهادی از روش رمزگذاری ECDLP استفاده کردند. با این وجود در مقابل حملات مرد میانی، حمله تکرار ،حمله جعل، حملات انکار سرویس و باران رنگین کمان آسیب پذیر می‌باشد. عبازاده و همکاران در سال ۲۰۲۱ طرح تبادل کلید امن را برای شبکه های مه پیشنهاد دادند[22] و در همان سال طرح بهبود یافته عبازاده توسط یاشار و همکاران پیشنهاد شد[23]. با این حال این طرح قابلیت احراز هویت ندارد و به همین دلیل برای سیستم های هواشناسس مناسب نیست. خواجه وند و همکاران در سال ۲۰۲۳ طراح احراز هویت امن برای خود روهای هوشمند را پیشنهاد دادند[24]، با اینکه این طرح از نظر امنیتی مقاوم در برابر حملات شناخته شد بود ولی برای سیستم های هواشناسی مناسب نیست. زینالی و همکاران در سال ۲۰۲۳ طرحی امن برای احراز هویت برای شبکه های اینترنت اشیا پیشنهاد دادن با اینکه این طرح در برابر حملات اکتیو و پسیو مقاوم است با این حال برای محیط های هواشناسی طراحی نشده است[25].

جدول ۱. مقایسه کارهای سوابق تحقیق

طرح	سال	اینترنت اشیا	بلاکچین	ایستگاه خودکار	نقاط ضعف
[11]	۲۰۱۶	✓	✓	x	هزینه محاسباتی بالا برای اعضای شبکه،عدم پشتیانی از ایستگاه‌های خودکار
[12]	۲۰۱۶	✓	✓	x	مصرف پهنای باند زیادی برای ذخیره داده‌ها ، عدم پشتیانی از ایستگاه‌های خودکار
[13]	۲۰۱۶	✓	✓	x	لغو مکانیسم‌های اجماع در شبکه‌های خصوصی و افزایش خطرات امنیتی
[14]	۲۰۱۷	✓	✓	x	حذف مفهوم Pow برای سرعت بخشیدن به کارایی تراکنش‌ها و عدم پشتیانی از ایستگاه‌های خودکار
[15]	۲۰۱۷	✓	✓	x	توان عملیاتی پایین بلاکچین اتریوم نمی‌تواند خواسته‌های سیستم اینترنت اشیا را برآورده کند و همچنین از ایستگاه‌های خودکار پشتیانی نمی‌کند.
[16]	۲۰۱۸	✓	✓	x	احتمال حملات انکار سرویس توزیع شده را افزایش می‌دهد و ایستگاه‌های خودکار را پوشش نمی‌دهد.

[17]	۲۰۱۸	✓	✓	x	نداشتن پیاده‌سازی دقیقی از روند طرح و عدم پوشش ایستگاه‌ها خودکار
[18]	۲۰۱۸	✓	✓	x	ناسازگاری با برنامه‌های بلادرنگ و عدم پوشش ایستگاه‌های خودکار.
[19]	۲۰۱۸	✓	✓	x	حملات افشای مخفی ،حمله تکرار ،قابلیت ردیابی،و استفاده مجدد از توکن و عدم پشتیانی از ایستگاه‌های خودکار
[20]	۲۰۲۰	x	✓	x	کلید نشست نابرابر طرفین، حمله تکرار و عدم پوشش ایستگاه‌های خودکار.
[21]	۲۰۲۰	✓	✓	x	حملات مرد میانی، حمله تکرار ، حمله جعل، حملات انکار سرویس ، باران رنگین کمان و عدم پوشش ایستگاه‌های خودکار.
[22]	۲۰۲۱	✓	✓	x	عدم پوشش ایستگاه‌های خودکار
[23]	۲۰۲۱	✓	✓	x	عدم پوشش ایستگاه‌های خودکار
[24]	۲۰۲۳	✓	✓	x	عدم پوشش ایستگاه‌های خودکار
[25]	۲۰۲۳	✓	✓	x	عدم پوشش ایستگاه‌های خودکار

۵. طرح پیشنهادی

این بخش مراحل طرح پیشنهادی را مطرح می‌کند. طرح پیشنهادی از سه بخش احراز هویت ، سیاست های دسترسی و توکن دسترسی تشکیل شده است که به ترتیب در این بخش بیان می‌شود.

طرح پیشنهادی ابتدا در یک کانال امن CPS و BCG در آغاز ارتباط فقط برای یک بار،کلیدهای عمومی خود را رد و بدل می‌کنند و آنها روی خم بیضویE و نقطهٔ $P \in E$ به توافق می‌رسند وE و P را منتشر می‌کنند. دلیل استفاده از کلید عمومی برای احراز هویت و جلوگیری از حملات مرد میانی می‌باشد. امنیت این روش بر سختی محاسبه مسئلهٔ لگاریتم گسسته در خم-های بیضوی استوار می‌باشد. به دلیل سرعت بیشتر و مصرف حافظه کم تر در رمزگذاری ECDLP (مشکل لگاریتم گسسته منحنی بیضی) نسبت به RSA از این روش رمزگذاری استفاده می‌کنیم.

۵-۱. نمادها

جدول ۲ نمادهای استفاده شده در طرح پیشنهادی را نشان می‌دهد.

جدول ۲. خلاصه‌ای از نمادهای استفاده شده در طرح پیشنهادی

نماد	توضیحات
CPS	سیستم پردازش داده
BCG	دروازه واسط بین CPSو AWS برای شبکه بلاک چین
AWS	ایستگاه خودکار
Q_s	کلید عمومی BCG
K_s	کلید خصوصی BCG
H	تابع درهم‌ساز
a	یک عدد تصادفی $a \in (1,q)$
b	یک عدد تصادفی $b \in (1,q)$
ID_i	شناسه کاربر $CPS_i's$
SK_{abcg}	کلید مشترک بین BCG و AWS
SK_{cbcg}	کلید مشترک بین CPS و BCG
$E_K(.)$	تابع رمزگذاری متقارن
$D_K(.)$	تابع رمزگشایی متقارن
P_j	خط‌مشی ایستگاه

PP_j	رضایت خطمشی P_j
T_{ij}	مهر زمانی
q	یک عدد اول بزرگ
GF_q	میدان متناهی F_q
$E(GF_q)$	خم بیضوی روی میدان متناهیF_q
P	نقطه P که $P\in E(GFq)$ بر اساس مقدار q
r_c,r_a,r_b	اعداد تصادفی تولید شده به ترتیب توسط CPS، AWS و BCG
TID_{ij}	آدرس تراکنش اضافه شده به بلاکچین به دلیل پذیرش خطمشی p_j توسط سیستم CPS_i
N_i	اعداد تصادفی
r_i	اعداد تصادفی
||	عملگر الحاق

۵-۲. احراز هویت

مراحل احراز هویت طرح پیشنهادی به شرح زیر می‌باشد:

۵-۲-۱. مرحله راه‌اندازی. در این مرحله BCG چند پارامتر برای ایجاد ارتباط با CPS ایجاد می‌کند.

BCG ابتدا یک عدد اول بزرگ با نام q انتخاب می‌کند، انتخاب E(GFq)یک گروه منحنی بیضوی که روی یک میدان محدود تعریف شده، نقطه P که $P \in E(GFq)$ که بر اساس مقدار q انتخاب می‌شود و تابع هش رمزنگاری h(.)سپس BCG یک عدد صحیح به نام$Ks \in (1;q)$ را به عنوان کلید مخفی خود انتخاب و کلید عمومی خودش را با فرمول Qs=KsP محاسبه می‌کند. در مرحله آخر BCG تمام پارامترهای انتخاب شده را به جز کلید مخفی خود(Ks) منتشر می‌کند.

۵-۲-۲. سیاست دسترسی

در مرحله اول CPS باید سیاست های دسترسی AWS (Pj) را پیدا کرده و با آنها موافقت کند.مراحل رابطه ۲-۱-۴ مراحل تائید سیاست دسترسی را نشان می‌دهد:

i. ابتدا CPS عدد تصادفی به نام a ($a \in (1,q)$) را انتخاب می‌کند و این عدد باید نزد CPS مخفی نگه داشته شود.در ادامه CPS مقدار X را به صورت X=aP محاسبه می‌کند و حاصل را با مهر زمانی T1 و یک عدد تصادفی با نام N1 الحاق نموده (Ai) و حاصل را توسط تابع هش،هش می‌کند و در HAi قرار می‌دهد و مقادیر Ai و HAi الحاق و در SA قرار می‌دهد و SAرا برای BCG ارسال می‌کند. رابطه ۱ مقادیر ایجاد شده را نمایش می‌دهد:

Generate random number a
X=aP
TS1=Timestamp (۱)
Generate a nonce N1
Ai=X ,TS1,N1
HAi=h (Ai)
SA= HAi || Ai

BCG ابتدا با استفاده از تابع هش ، حاصل هش Ai را به دست می‌آورد و حاصل را با مقدار HAi مقایسه می‌کند و در صورت صحت پیام، اعتبار پیام را با مقایسه زمان فعلی و T1 ارسالی بررسی می‌کند. رابطه ۲ مقادیر ایجاد شده را نمایش می‌دهد:

Ai′=h(Ai)
If Ai′≠HAi:break (۲)
If Time >TS1 :break;

در صورت اعتبار پیام، BCG یک عدد تصادفی به نام b $\in(1,q),b$ را انتخاب می‌کند و این عدد باید نزد BCG مخفی نگه داشته شود. در ادامه BCG مقدار Y را به صورت Y=bP محاسبه می‌کند. BCG با استفاده از X وb ،کلید مشترک بین خود و CPS با نام K را به شکل رابطه ۳ محاسبه می‌کند:

K= bX (۳)

سپس BCG مقادیر مهر زمانی T2 و یک عدد تصادفی با نام N2را محاسبه می‌نماید و با مقدار Y الحاق نموده و در Bi قرار می‌دهد،رابطه ۴ مقدار Bi را نمایش می‌دهد:

Bi = Y,TS2,N2 (۴)

و در ادامه مقدار HBi با استفاده از تابع هش طبق رابطه ۵ تولید می‌شود:

$$HBi=H(K,BCG_{pr}X,TS2,N2) \quad (۵)$$

و در نهایت مقدار BCG مقادیر Bi و HBi الحاق و در SB قرار می‌دهد و SB را برای CPS ارسال می‌کند، رابطه ۶ مقدار SB را نمایش می‌دهد:

$$SB= HBi \,||\, Bi \quad (۶)$$

هنگامی که CPS پیام را دریافت کرد، CPS کلید K را با فرمول K=aY محاسبه می‌کند. سپس با استفاده از تابع هش ، حاصل هش Bi′ را به دست می‌آورد و مقدار به دست آمده را با مقدار HBi مقایسه می‌کند و در صورت صحت پیام، اعتبار پیام را با مقایسه زمان فعلی و T2 ارسالی را بررسی می‌کند.رابطه ۷ مقادیر ایجاد شده را نمایش می‌دهد:

$$Bi'=H(K||aBCG_{pc}||TS2||N2) \quad (۷)$$

If Bi′≠HBi:break;
If Time >TS2 :break;

در صورت معتبر بودن پیغام،CPS مقادیر Pj,PPj,IDi را با عدد تصادفی N3 و مهر زمانی (T3) الحاق کرده و توسط تابع هش،هش می‌کند و طبق رابطه ۸ در HCi قرار می‌دهد:

$$HCi=H(ID_i,P_j,PP_j,TS3,N3 \quad (۸)$$

و در آخر مقادیر HCi,IDi,Pj,PPj,TS3,N3 را با هم الحاق و با کلید K رمزنگاری و در SC قرار می‌دهد و SC را طبق رابطه ۹ برای BCG ارسال می‌کند:

$$SC=E_K(HCi,ID_i,P_j,PP_j,TS3,N3) \quad (۹)$$

iv.هنگامی که BCG پیام را دریافت کرد،پیام رمز شده SC را با کلید k رمزگشایی می‌کند و اعتبار پیام را با مقایسه زمان فعلی و T3 ارسالی را بررسی می‌کند در صورت صحت پیام،با استفاده از تابع هش، حاصل هش Ci′ را به دست می‌آورد و مقدار به دست آمده را با مقدار HCi مقایسه می‌کند. رابطه ۱۰ مقادیر ایجاد شده را نمایش می‌دهد:

If Time >T3 :break; (۱۰)

$DC=D_k(SC)$
$Ci'=H(ID_i|,P_j, PP_j,TS3 ,N3)$
If Ci′≠HCi:break;

در صورت معتبر بودن پیام،BCG کلید مشترک بین CPS و BCG یعنی (SKcbcg) با استفاده از رابطه ۱۱ ایجاد می‌شود:

$$TS4= Timestamp \quad (۱۱)$$

$$SK_{cbcg} = H(ID_i,TS4,X,Y)$$

این کلید در پیام‌های بعدی استفاده می‌شود.

V. Pj، PPj و IDi با استفاده از کلید تولید شده رمزگذاری شده به عنوان یک تراکنش در زنجیره بلاک ذخیره می‌شوند. در مرحله آخر آدرس تراکنش (TIDij) به همراه (SKcbcg) و عدد تصادفی N4 و یک مهر زمانی (T5) با استفاده از کلید مشترک بین BCG و CPS یعنی K رمزگذاری و طبق رابطه ۱۲ به CPS ارسال می‌شود:

$$SD=E_k(SK_{cbcg}|| TID_{ij}|| T5 || N4) \quad (۱۲)$$

شکل ۳ مرحله تائید سیاست دسترسی در طرح پیشنهادی را نشان می‌دهد.

CPS_i	BCG	Blockchain Network	Smart contract for the gateway
Choose a ∈(1, q) X=aP TS1= Timestamp Generate a nonce N1 Ai=X, TS1, N1 HAi=h (Ai) SA= HAi ||Ai SA send to BCG SA →	Ai'=h(Ai) If Ai'≠ HAi: break; If Time >TS1: break; Choose b ∈(1, q) Y=bP K=bX TS2= Timestamp Generate a nonce N2 Bi= Y, TS2, N2 HBi=h(K, BCGprX,TS2,N2) SB= HBi || Bi SB send to CPS_i ← SB		
K=aY Bi'=h(K||aBCGpc||TS2||N) if Bi'≠HBi:break; If Time >TS2: break; Generate a nonce N3 TS3= Timestamp HCi=h (ID_i, P_j, PP_j, TS3, N3) SC=EK (HCi, ID_i, P_j, PP_j, TS, N3) SC send to BCG SC →	DC=Dk (SC) If Time >TS3: break; Ci'=h (IDi|,P_j, PP_j,TS3 ,N3) If Ci'≠HCi: break; TS4= Timestamp SK_{cbcg}=h (ID_i, TS4, X, Y) EM=$E_{SK_{cbcg}}$(PP_j, P_j, ID_i) Em send to Blockchain Network for Store Em →	Add Transaction in blockchain and return transaction ID (TID_{ij}) TID_{ij} send to BCG ← TID_{ii}	
	Invoke Log (TIDij) Function in gateway Smart contract Send TIDij to CPS_i with Generated secretkey(SK_{cbcg}) Between BCG and CPS Generate a nonce N4 TS5= Timestamp SD=Ek (SK_{cbcg}, TID_{ij}, TS5, N4) SD send to CPS_i ← SD	Invoke →	

شکل (۳): مرحله تائید سیاست دسترسی

۵-۲-۳. توکن دسترسی

مراحل زیر دسترسی CPS به AWS را شرح می‌دهد :

CPS ابتدا مقدار رابطه ۱۳ را تولید می‌کند:

$$PP_j = E_{SK_{cbcg}}(TID_{ij} \,||\, r_c) \quad (۱۳)$$

که در آن TIDij ،rc و SKcbcg به ترتیب شماره تراکنش مرتبط با پذیرش خط مشی‌های AWS، یک عدد تصادفی و یک کلید مخفی مشترک بین خود و BCG هستند. CPS (PPj, rc) را به AWS ارسال می‌کند.

ii.هنگامی که AWS پیام را دریافت کرد، یک عدد تصادفی (ra) تولید می‌کند و مقدار رابطه ۱۴ را محاسبه می‌کند:

$$M_{sig} = HMAC(r_c \,||r_a \,||\, PP_j, SK_{abcg}) \quad (۱۴)$$

و مقادیر رابطه ۱۵ را به BCG می‌فرستد:

$$(M_{sig}, r_a, r_c, PP_j) \quad (۱۵)$$

iii.پس از دریافت پیام، BCG یک امضا طبق رابطه ۱۶ تولید می‌کند:

$$M'_{sig} = HMAC(r_c \,||r_a \,||PP_j, SK_{abcg}) \quad (۱۶)$$

و آن را با امضای دریافتی مقایسه می‌کند (Msig). ادامه طرح به شرط رضایت بخش M′sig=Msig مربوط می‌شود. BCG ،PPj را رمزگشایی می‌کند و ادعای CPS را با استفاده از شبکه بلاکچین تضمین می‌کند. در مرحله بعد، BCG یک عدد تصادفی دیگر (rb) و مقدار رابطه ۱۷ را تولید می‌کند:

$$M''_{sig} = HMAC(r_b \,||\, r_c \,||\, TID_{ij}, SK_{cbcg}) \quad (۱۷)$$

و در نهایت (M″sig, rb) را برای CPS ارسال می‌کند.

iv.هنگامی که CPS پیام (M″sig, rb) را دریافت کرد، اعتبار BCG را از رابطه ۱۸ بررسی می‌کند:

$$M''_{sig} == HMAC(r_b \,||\, r_c \,||\, TID_{ij}, SK_{cbcg}) \quad (۱۸)$$

CPS از قبل مقدارrc ،TIDijو SKcbcg را می‌داند. ادامه طرح مشروط به امضای تولید شده CPS و امضای BCG است.در ادامه، CPS یک پیام امضا شده به طبق رابطه ۱۹ تولید کرده و آن را به BCG می‌فرستد.

$$N_{sig} = HMAC(r_b, SK_{cbcg}) \quad (۱۹)$$

V. درستی رابطه ۲۰ توسط BCG بررسی می‌شود :

$$N_{sig} = ? \; N'_{sig} \quad (۲۰)$$

و مقدار N′sig توسط رابطه ۲۱ تولید می‌شود:

$$N'_{sig} = HMAC(r_b, SK_{cbcg}) \quad (۲۱)$$

در صورت تساوی مقادیر،BCG توکن دسترسی را طبق رابطه ۲۲ محاسبه و برای CPS ارسال می‌کند.

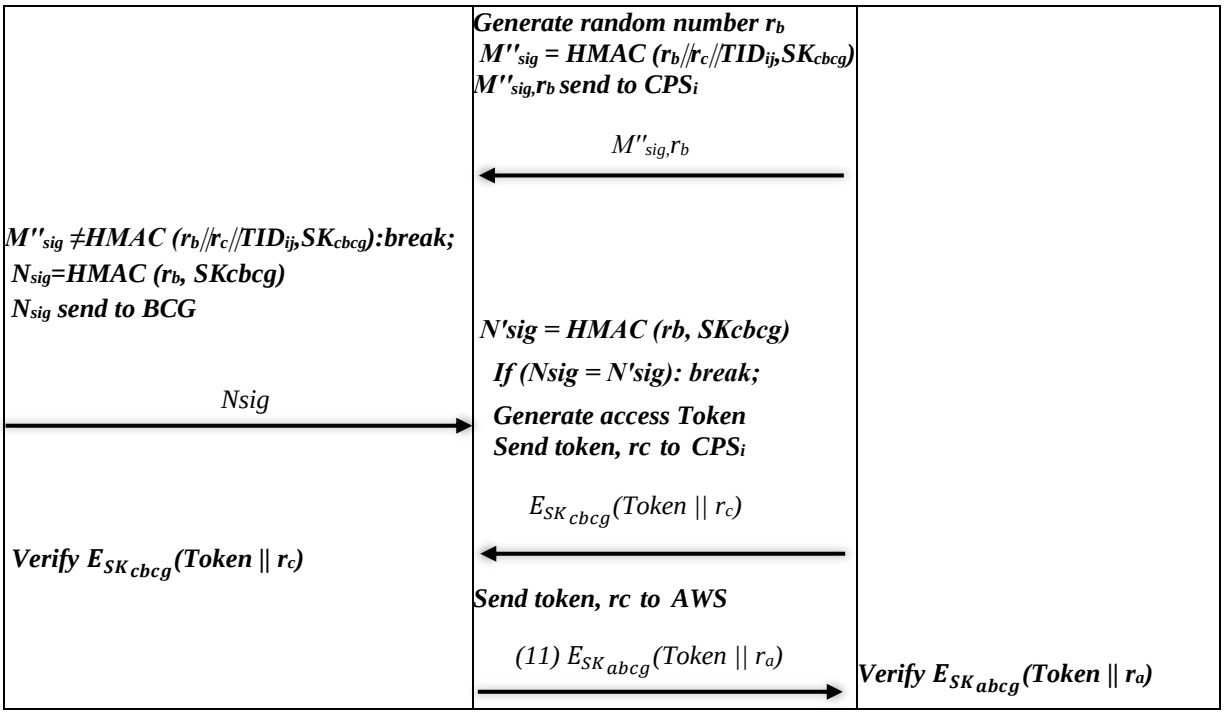
$$E_{SK_{cbcg}}(Token \,||\, r_c) \quad (۲۲)$$

همچنین توکن دسترسی را طبق رابطه ۲۳ برای AWS ارسال می‌کند.

$$E_{SK_{abcg}}(Token \,||\, r_a) \quad (۲۳)$$

زمانی که CPS پیام $E_{SK_{cbcg}}$ (Token || rc) را دریافت کرد آن را با کلید SKcbcg رمزگشایی می‌کند.اگر rc به دست آمده برابر با مقدار CPS باشد،CPS به توکن دریافتی اعتماد می‌کند. همین امر برای AWS نیز صادق است. شکل ۴ مرحله ایجاد توکن دسترسی نشان می‌دهد.

CPS_i	BCG	AWS
Generate random number r_c ***$PP_j = SKcbcg\ (TID_{ij} // r_c)$*** ***$PP_j$, rc send to AWS*** ***$PP_j$, rc send to AWS*** PP_j, rc →		***Generate random number r_a*** ***$M_{sig} = HMAC\ (r_c, r_a, PP_j, SK_{abcg})$*** ***$M_{sig}$, r_a,r_c,PP_j send to BCG*** (M_{sig}, r_a, r_c, PPj) ←
	M'_{sig}=HMAC (r_c, r_a,PP_j,SK_{abcg}) ***If (Msig ≠ M'sig): break;*** ***Find PP_j and verify it according to blockchain transaction (the connection with blockchain is done through RPC protocol)***	



شکل ۴. مرحله ایجاد توکن دسترسی

٦. تجزیه و تحلیل امنیتی

در این بخش، امنیت و هزینه‌های طرح پیشنهادی بررسی می‌شود. برای تحلیل امنیت ابتدا حملات شایع درزمینهٔ ی شبکه‌های هواشناسی بررسی شده و نشان داده خواهد شد که طرح پیشنهادی در برابر این حملات مقاوم است. در گام بعدی با استفاده از ابزار AVISPA طرح پیشنهادی تحلیل شده و نتیجه‌ی این شبیه سازی نیز امنیت طرح پیشنهادی را نشان می‌دهد.

٦-١. ارزیابی امنیتی غیر رسمی طرح پیشنهادی

در این بخش مقاومت طرح در برابر حملات موجود بررسی خواهد شد. در این بخش به صورت غیر رسمی اثبات می‌کنیم که طرح در مقابل حملات مرد میانی، حمله‌ی جعل هویت و حمله‌ی تکرار و حمله افشای مخفی ، حمله قابلیت ردیابی ،حمله جست‌وجوی فراگیر و حمله انکار سرویس مقاوم است.تحلیل غیررسمی مبتنی بر دانش و خلاقیت تحلیلگر است

٦-١-١. حمله تکرار

از آنجایی که در طرح پیشنهادی در مرحله تائید سیاست دسترسی ، برای پیام‌های رد و بدل شده از مهر زمانی و عدد تصادفی استفاده می‌شود و در مرحله ایجاد توکن تمامی اعضای شبکه در مرحله ساخت توکن دسترسی شرکت می‌کنند، امکان حمله تکرار حذف می‌شود. وجود مقادیر مخفی مشترک (SKabcg،SKcbcg) بین طرف‌های طرح و استفاده از مقادیر تازه تصادفی (N1,N2,N3,N4, ,rc, ra, rb) و استفاده از مهرهای زمانی (TS1,TS2,TS3,TS4,T5) توسط طرف‌های طرح باعث می‌شود که پیام‌های هر جلسه با پیام‌های جلسات قبلی متفاوت باشد. در نتیجه، احتمال حمله تکرار از بین می‌رود.

٦-١-٢. مقاومت در برابر حمله افشای مخفی

در مرحله تائید سیاست دسترسی پیام‌های مهم ارسال شده بین CPS و BCG توسط یک کلید مشترک رمزگذاری می‌شوند، مانند SKcbcgوTIDij که به صورت رابطه ۱ رمزگذاری شده است:

$$E_k(SK_{cbcg} || TID_{ij} || TS5,N4) \quad (۱۱)$$

در مرحله ساخت توکن دسترسی پیام‌های مهم ارسال شده بین CPS و BCG توسط یک کلید مشترک رمزگذاری می‌شوند، مانند توکن که به صورت رابطه ۲ رمزگذاری شده است:

$$E_{SK_{cbcg}} (Token || r_c) \quad (۲۲)$$

همچنین پیام‌های مهم ارسال شده بینAWS وBCG مانند توکن را با استفاده از یک مقدار مخفی مشترک، به شکل رابطه ۳ رمزگذاری می‌کنیم.

$$E_{SK_{abcg}}(Token||\ r_a) \quad (۲۳)$$

به دلیل رمزگذاری پیام‌ها در جلسه، اطلاعات مهم محرمانه می‌ماند.همچنین وجود مقادیر مخفی مشترک به اعضای طرح اجازه می‌دهد تا کد احراز هویت پیام مانند Msig و Nsig را تولید کنند تا بتوانند یکدیگر را احراز هویت کنند و از ارسال داده‌ها به طرف غیرمجاز خودداری کنند.

٦-١-٣. مقاومت در برابر حمله قابلیت ردیابی

همان‌طور که قبلاً ذکر شد، به دلیل دخالت اعداد تصادفی در تمام پیام‌های منتقل‌شده و تغییر این اعداد تصادفی در هر جلسه، مهاجم نمی‌تواند مقدار ثابتی پیدا کند. در نتیجه، مهاجم قادر به ردیابی طرف‌های طرح با استفاده از پیام‌های انتقال یافته طرح نیست. همچنین، به دلیل عدم ارتباط بین پیام‌های ارسال شده در هر جلسه، مهاجم نمی‌تواند با استراق سمع پیام‌های منتقل‌شده قبلی، داده‌ای را در جلسه جاری فاش کند.

٦-١-٤. عدم پیوند ایستگاه

در طرح پیشنهادی، برای هر AWS یک کلید جداگانه صادر می‌کنیم. هر CPS ملزم به پردازش، پذیرش مرحله خط‌مشی‌ها و ایجاد مرحله توکن دسترسی برای استفاده مستقل از هر AWS است. می‌توان گفت که CPS برای هر ایستگاه از یک توکن جداگانه استفاده می‌کند، بنابراین با افشای یک توکن، سایر ایستگاه‌ها تهدید نمی‌شوند.

٦-١-٥. مقاومت در برابر حملات مرد میانی

در مرحله تائید سیاست دسترسی کلید مخفی Ks برای جلوگیری از حمله مرد میانی استفاده می‌شود و مهاجم نمی‌تواند برای رهگیری داده‌های مبادله شده و تزریق اطلاعات نادرست در ارتباط بین BCG و CPS نفوذ کند.همچنین در مرحله ساخت توکن دسترسی وجود مقادیر مخفی مشترک به اعضای طرح اجازه می‌دهد تا کد احراز هویت پیام مانند Msig و Nsig را تولید کنند تا بتوانند یکدیگر را احراز هویت کنند و از ارسال داده‌ها به طرف غیرمجاز خودداری کنند.

٦-١-٦. مقاومت در برابر جست‌وجوی فراگیر

به دلیل دخالت اعداد تصادفی در تمام پیام‌های منتقل‌شده و تغییر این اعداد تصادفی در هر جلسه، مهاجم نمی‌تواند مقدار ثابتی پیدا کند و حملات جست‌وجوی فراگیر خنثی می‌شود.

٦-١-٧. مقاومت در برابر حمله انکار سرویس

دلیل استفاده از بلاکچین، معماری سیستم به سمت معماری توزیع شده حرکت می کند. توزیع یک سیستم احتمال حمله انکار سرویس را کاهش می دهد. با این حال، به دلیل عدم مشارکت ایستگاهای هواشناسی AWSدر شبکه بلاکچین و CPSهای متصل به شبکه بلاکچین توسط BCG، توزیع سیستم کاهش می یابد. AWS ها نمی توانند مستقیماً در شبکه بلاکچین شرکت کنند، زیرا منابع زیادی برای این منظور مورد نیاز است. با توجه به استفاده از بلاکچین به عنوان شخص ثالث قابل اعتماد (TTP) و AWS ها بین BCG های مختلف، احتمال حمله انکار سرویس به سیستم کاهش می یابد. همچنین با توجه به عدم تغییر کلیدها در هر جلسه و وجود کلیدهای مختلف به ازای هر CPS برای هر ایستگاه هواشناسی، امکان تغییر مقادیر و همگام سازی سیستم از بین می رود.

٦-٢. تجزیه و تحلیل امنیت رسمی

ابزار AVISPA یک شبیه سازی رسمی برای ارزیابی اینکه آیا یک طرح ایمن یا ناامن است می‌باشد[26].AVISPA ابزاری است برای اعتبارسنجی خودکار طرح‌ها و برنامه‌های کاربردی که از لحاظ امنیتی حساس می‌باشند[27]. طرح‌ها برای بررسی شدن توسط این ابزار بایستی به زبان HLPSL پیاده سازی شوند[28]. این زبان بر پایه‌ی نقش است. نقش‌های اصلی برای نشان دادن نقش شرکت کننده و نقش‌های ترکیبی برای شرح سناریو و عملکرد هر کدام از نقش‌های اصلی در روند اجرای طرح. هر نقش از نقش دیگر مستقل بوده و اطلاعات اولیه‌ای را به عنوان پارامتر دریافت می کند و از طریق کانال با دیگر نقش‌ها در ارتباط می‌باشد.

کانال‌های موجود در این ابزار به چند دسته تقسیم می‌شود که در حال حاضر فقط کانال (Dolev-Yao) توسط این ابزار پشتیبانی شده و نوع کانال ناامن می‌باشد[29]. نقش‌ها پروسه‌های مستقل هستند، دارای نام بوده و توسط پارامترها اطلاعاتی دریافت کرده و شامل تعاریف محلی می‌باشند. قالب خروجی این زبان به‌وسیله‌ی یکی از چهار پشته‌ی بررسی‌کننده‌ی مدل سریع (OFMC)، منطق محدودیت بر اساس جست‌وجوگر حمله

(CL-AtSe)، بررسی کننده مدل ست (SATMC) و تقریب خودکار برای بررسی امنیت طرح‌ها بر مبنای ماشین خودکار درختی(TA4SP) تولید می‌گردد.

۶-۲-۱. تجزیه و تحلیل نتایج شبیه سازی

ابزار AVISPA، نشان می‌دهد. .شکل ۵ و ۶ به ترتیب، نتایج شبیه سازی طرح پیشنهادی برای مرحله تائید دسترسی و شکل‌های ۷ و ۸ به ترتیب نتایج شبیه سازی برای مرحله ایجاد توکن دسترسی تحت OFMC و AtSe-CL را نشان می‌دهد. نتایج تجزیه و تحلیل امنیتی نشان می‌دهد که طرح پیشنهادی ایمن است.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/faz-access.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime:0.00s
  searchTime:0.13s
  visitedNodes:128 nodes
  depth: 4 plies
```

شکل (۵): نتایج شبیه سازی تائید دسترسی با ابزارOFMC

```
SUMMARY
SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL
PROTOCOL
/home/span/span/testsuite/results/faz-access.if
GOAL
 As Specified
BACKEND
 CL-AtSe
STATISTICS
  Analysed   : 12 states
  Reachable  : 26 states
  Translation: 0.00 seconds
  Computation: 0.00 seconds
```

شکل (۶): نتایج شبیه سازی مرحله تائید دسترسی با ابزار CL-AtSe

```
%OFMC
%Version of 2006/02/13
SUMMARY
SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/ home/span/span/testsuite/results/faz-2.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 0.91s
 visitedNodes: 1286 nodes
 depth: 7 plies
```

شکل(۷):نتایج شبیه سازی توکن دسترسی با OFMC

```
SUMMARY
SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL
PROTOCOL
/home/span/span/testsuite/results/faz-2.if
GOAL
 As Specified
BACKEND
 CL-AtSe
STATISTICS
  Analysed   : 10 states
  Reachable  : 23 states
  Translation: 0.00 seconds
  Computation: 0.00 seconds
```

شکل(۸): نتایج شبیه سازی مرحله توکن دسترسی با CL-AtSe

۷. ارزیابی طرح پیشنهادی

در این بخش، تحلیل عملکرد طرح پیشنهادی و الزامات امنیتی با طرح یاوری و همکاران مقایسه شده است. نمادهای زیر برای ارزیابی هزینه محاسباتی طرح پیشنهادی تعریف شده است. Th تعداد اجرای عملیات هش است. Pe تعداد اجرای رمزگذاری کلید عمومی است. Pd تعداد اجرای رمزگشایی کلید عمومی

است. Se تعداد اجرای رمزگذاری کلید متقارن است. Sd عدد اجرای رمزگشایی کلید متقارن است. Tn تعداد اجرای عملیات تولید اعداد تصادفی می‌باشد.Tm تعداد اجرای تابع HMAC می‌باشد. زمان اجرا عملیات مختلف بر اساس مرجع ۱۲ می‌باشد. جدول ۳ زمان اجرای عملیات‌های تعریف شده را بر اساس میلی ثانیه نشان می‌دهد.

جدول (۳): زمان اجرا برای عملیات محاسباتی

عملیات	زمان اجرا(میلی ثانیه)
Th	**0.0023**
Pe	**3.8500**
Pd	**3.8500**
Se	**0.0046**
Sd	**0.0046**
Tn	**0.539**
Tm	**0.0046**

۷-۱. هزینه محاسباتی

جداول ۴ و ۵ مقایسه‌ای از هزینه محاسباتی طرح پیشنهادی با یاوری و همکاران را نشان می‌دهد. هزینه کل طرح یاوری و همکاران 2.7387 میلی ثانیه است. در مقابل، هزینه طرح پیشنهادی ما 4.3833 میلی ثانیه است. دلیل افزایش زمان اجرا ایجاد ارتباط بین CPS و BCG در کانال ناامن می‌باشد. برقراری تعادل بین امنیت و زمان اجرا با توجه به رخنه‌های امنیتی و حملات، کاری دشوار خواهد بود، بنابراین در نهایت برای تضمین امنیت الزامی است که زمان اجرا از اهمیت کمتری برخوردار شود و طرح پیشنهادی دارای زمانی اجرای بالاتری باشد .لازم به این نکته ضروری می‌باشد درحالی که هزینه طرح پیشنهادی ما بیش تر از طرح یاوری و همکاران می‌باشد اما هم در مرحله تائید دسترسی نیاز به کانال امن نیست و هم مشکلات امنیتی مطرح شده برای طرح یاوری و همکاران را نداریم.

جدول (۴): مقایسه زمان اجرا برای مرحله تائید سیاست دسترسی

نوع توابع	BSAMS	IBCbAP
رمزنگاری کلید مشترک(K)	2Se	1Se
رمزگشایی کلید مشترک(K)	2Sd	0
تابع هش	7Th	1Th
تولید اعداد تصادفی	4Tn	1Tn
مجموع	2.1905ms	0.5459ms

جدول (۵): مقایسه زمان اجرا برای مرحله ایجاد توکن دسترسی

نوع توابع	BSAMS	IBCbAP
رمزنگاری کلید مشترک(K)	3Se	3Se
رمزگشایی کلید مشترک(K)	1Sd	1Sd
HMAC	4Tm	4Tm
تولید اعداد تصادفی	4Tn	4Tn
مجموع	2.1928ms	2.1928ms

۸. نتیجه‌گیری

ما در این مقاله یک طرح احراز هویت متقابل مبتنی بر شبکه بلاکچین را برای سیستم‌های هواشناسی پیشنهاد دادیم. طرح پیشنهادی از بخش احراز هویت متقابل و سیاست دسترسی و تولید توکن تشکیل شده است که باعث می‌شود ارتباط ایمن بین تجهیزات هواشناسی ایجاد شود. نتایج تجزیه تحلیل امنیت طرح پیشنهادی به صورت رسمی و غیر رسمی نشان داده که طرح پیشنهادی در برابر حملات اکتیو و پسیو مقاوم است. همچنین ارزیابی طرح پیشنهادی نشان می‌دهد که به خاطر افزایش امنیت در طرح پیشنهادی هزینه پردازشی نسبت به سایر طرح‌های مشابه بیشتر است. هدف ما در آینده ارائه روش‌های احراز هویت و تبادل کلید سبک وزن مبتنی بر بلاکچین برای سیستم‌های هواشناسی است.

منابع

[1] Y. Salami and V. Khajehvand, “SMAK-IOV: Secure Mutual Authentication Scheme and Key Exchange Protocol in Fog Based IoV,” *J. Comput. Robot.*, vol. 13, no. 1, pp. 11–20, 2020.

[2] A. Ghaffari, “Designing a wireless sensor network for ocean status notification system,” *Indian J. Sci. Technol.*, vol. 7, no. 6, p. 809, 2014.

[3] A. Ghaffari, “Congestion control mechanisms in wireless sensor networks: A survey,” *J. Netw. Comput. Appl.*, vol. 52, pp. 101–115, 2015.

[4] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, “Security of internet of things based on cryptographic algorithms: a survey,” *Wirel. Networks*, vol. 27, pp. 1515–1555, 2021.

[5] Y. Salami, V. Khajevand, and E. Zeinali, “Cryptographic Algorithms: A Review of the Literature, Weaknesses and Open Challenges,” *J. Comput. Robot.*, vol. 16, no. 2, pp. 46–56, 2023.

[6] Y. Salami, F. Taherkhani, Y. Ebazadeh, M. Nemati, V. Khajehvand, and E. Zeinali, “Blockchain-Based Internet of Vehicles in Green Smart City: Applications and Challenges and Solutions,” *Anthropog. Pollut.*, vol. 7, no. 1, 2023.

[7] H. Han, R. K. Shiwakoti, R. Jarvis, C. Mordi, and D. Botchie, “Accounting and auditing with blockchain technology and artificial Intelligence: A literature review,” *Int. J. Account. Inf. Syst.*, vol. 48, p. 100598, 2023.

[8] T. Huynh-The *et al.*, “Blockchain for the metaverse: A Review,” *Futur. Gener. Comput. Syst.*, 2023.

[9] A. Pasdar, Y. C. Lee, and Z. Dong, “Connect API with blockchain: A survey on blockchain oracle implementation,” *ACM Comput. Surv.*, vol. 55, no. 10, pp. 1–39, 2023.

[10] T. M. Tan and S. Saraniemi, “Trust in blockchain-enabled exchanges: Future directions in blockchain marketing,” *J. Acad. Mark. Sci.*, vol. 51, no. 4, pp. 914–939, 2023.

[11] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, “FairAccess: a new Blockchain-based access control framework for the Internet of Things,” *Secur. Commun. Networks*, vol. 9, no. 18, pp. 5943–5964, 2016, doi: 10.1002/sec.1748.

[12] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, “World of empowered IoT users,” *Proc. - 2016 IEEE 1st Int. Conf. Internet-of-Things Des. Implementation, IoTDI 2016*, pp. 13–24, 2016, doi: 10.1109/IoTDI.2015.39.

[13] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[14] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “LSB: A Lightweight Scalable Blockchain for IoT security and anonymity,” *J. Parallel Distrib. Comput.*, vol. 134, pp. 180–197, 2019, doi: 10.1016/j.jpdc.2019.08.005.

[15] K. R. Özyilmaz and A. Yurdakul, “Work-in-progress: Integrating low-power IoT devices to a Blockchain-Based Infrastructure,” *Proc. 13th ACM Int. Conf. Embed. Softw. 2017 Companion, EMSOFT 2017*, 2017, doi: 10.1145/3125503.3125628.

[16] M. K. Kebede and S. K. Pani, “Reshaping IOT Through Blockchain,” *Proc. 3rd Int. Conf. I-SMAC IoT Soc. Mobile, Anal. Cloud, I-SMAC 2019*, pp. 1–5, 2019, doi: 10.1109/I-SMAC47947.2019.9032442.

[17] O. Novo, “Blockchain meets IoT: An architecture for scalable access

management in IoT," *IEEE internet things J.*, vol. 5, no. 2, pp. 1184–1195, 2018.

[18] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, 2018, doi: 10.1016/j.cose.2018.06.004.

[19] S. C. Cha, J. F. Chen, C. Su, and K. H. Yeh, "A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things," *IEEE Access*, vol. 6, no. c, pp. 24639–24649, 2018, doi: 10.1109/ACCESS.2018.2799942.

[20] S. Rostampour, M. Safkhani, Y. Bendavid, and N. Bagheri, "ECCbAP: A secure ECC-based authentication protocol for IoT edge devices," *Pervasive Mob. Comput.*, vol. 67, p. 101194, 2020, doi: 10.1016/j.pmcj.2020.101194.

[21] M. Yavari, M. Safkhani, S. Kumari, S. Kumar, and C. M. Chen, "An Improved Blockchain-Based Authentication Protocol for IoT Network Management," *Secur. Commun. Networks*, vol. 2020, 2020, doi: 10.1155/2020/8836214.

[22] Y. Salami, Y. Ebazadeh, and V. Khajehvand, "CE-SKE: cost-effective secure key exchange scheme in Fog Federation," *Iran J. Comput. Sci.*, vol. 4, no. 3, pp. 1–13, 2021.

[23] Y. Salami and V. Khajehvand, "LSKE: Lightweight Secure Key Exchange Scheme in Fog Federation," *Complexity*, vol. 2021, p. 4667586, 2021.

[24] Y. Salami, V. Khajehvand, and E. Zeinali, "SAIFC: A Secure Authentication Scheme for IOV Based on Fog-Cloud Federation," *Secur. Commun. Networks*, vol. 1, 2023.

[25] Y. Salami, V. Khajehvand, and E. Zeinali, "SOS-FCI: a secure offloading scheme in fog–cloud-based IoT," *J. Supercomput.*, pp. 1–31, 2023.

[26] "Avispa." http://www.avispa-project.org/

[27] Y. Salami, V. Khajehvand, and E. Zeinali, "E3C: A Tool for Evaluating Communication and Computation Costs in Authentication and Key Exchange Protocol," 2022, doi: 10.48550/ARXIV.2212.03308.

[28] D. Von Oheimb, "The high-level protocol specification language HLPSL developed in the EU project AVISPA," in *Proceedings of APPSEM 2005 workshop*, 2005, pp. 1–17.

[29] R. Küsters and T. Wilke, "Automata-Based Analysis of Recursive Cryptographic Protocols," in *STACS 2004*, 2004, pp. 382–393.